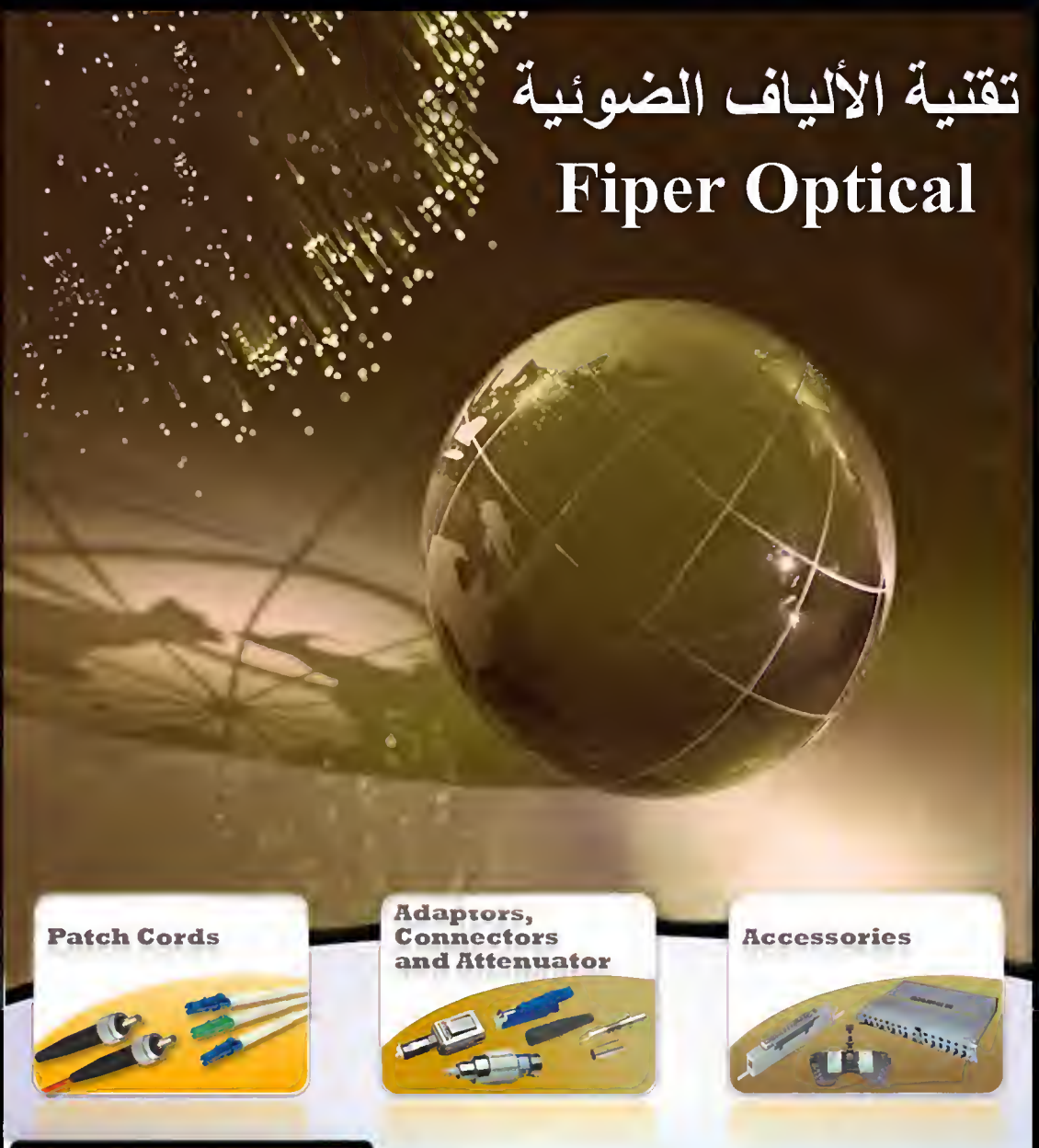
MAGAZINE
NETWORK SET
السنة الأولى - تشرين الأول /أكتوبر الموافق لعام 2010
أول مجلة عربية تختص بأمور الشبكات تصدر من موقع WWW.NetworkSet.net

تقنية الألياف الضوئية
Fiper Optical



- التطورات الأساسية في مجال الألياف الضوئية
- كيف تتم عملية نقل البيانات في الليف الضوئي
- أنواع وأشكال الكونيكتور

نتائج الأستفتاء

ماصلتك بعالم الشبكات ؟

- طالب 39%
- موظف 38%
- هاوي 19%
- زائر فقط 4%

networkset.net

تقرأون في هذا العدد

IGMP
Internet Group Management Protocol

شاهدوا أيضا أقسام

- مصطلحات تقنية
- عتاد ومعلومات
- مشاكل وحلول

7

أفتتاحية العدد

قيمة الوقت

دائما ماتصلني رسائل على البريد من أشخاص يريدون الدراسة والتعلم في مجال الشبكات لكن لديهم مشكلة صغيرة على حد تعبيرهم أنهم أصبحوا في عمر الثلاثين ويريدون أن يبدأوا التعلم والدراسة في هذا العمر وتختلف الرسائل أحيانا فمنهم من يقول أنه الآن في عمر الخامس والعشرين ومنهم من يقول أنه في الخامسة والثلاثين والخ....وحقيقة أنا أستغرب أحيانا من هذا التفكير الذي أعده بنظري تفكير سلبي إلى أبعد الحدود بسبب سوء تقدير هؤلاء الأشخاص إلى قيمة الوقت أولا وإلى سوء تقدير قدراتهم العقلية ثانيا لان الله أمنا علينا بهذه القدرة عن غيرنا من مخلوقات الأرض وهي العقل والتفكير وبقدرة غير محدودة وقد خطرت على بالي فكرة هذا المقال حقيقة عندما كتبت عن أكثر شخص حاصل على شهادة CCIE في العالم في العدد السابق من المجلة وهو كوري الأصل وأسمه Chang-Min هذا الكوري ببساطة أنتهى من شهاداته الرابعة في الـ CCIE ولم ينتظر اكثر من ثلاث أيام حتى يبدأ التجهيز للشهادة الخامسة ومن درس لهذه الشهادة يعلم مقدار الضغط الذي يحدث قبل وبعد الأمتحان ولكن هذا الكوري لم يعطي مجال كبير للراحة ولأضاعة الوقت بل على الفور أشترك في مجموعة على موقع سيسكو لدراسة الشهادة الخامسة وحصل عليها ولو نظرت إلى تاريخ حصوله على أول شهادة وآخرها لوجدت أنه خمس سنوات فقط كانت كافية لكي يصنف هذا الشخص ويعمل في هيئة علماء ومهندسي الكمبيوتر لان شهادة واحدة مثل هذه تعد مثل دراسة ماجستير أو دكتورة في الجامعة وطبعا انا أقصد المعنى الحقيقي لدراسة هذه الشهادة وليس الأطلاع على الأسئلة والتدريب على الأمتحان فقط .

ومن هنا أحببت أن أعود واسلط الضوء على حقيقة وقيمة الوقت في حياتنا فأنا أعتقد أن كل شخص فينا قادر على تغيير حياته ومستقبله في سنة واحدة فقط وليس خمس سنوات لكن لوفهمت الوقت وأحسنت تقديره ,وللوقت هناك شروط ومن أهم هذه الشروط هي خطة الدراسة وتنظيم الوقت فبدون خطة دراسة لن تستفيد من وقتك لان لو بدأت مثلا بدراسة أحد الشهادات أو بقراءة أحد الكتب ولم تضع وقت معين للانتهاء منه إذا أنت أضعت منك الكثير من الوقت وطبعا هذا يعود إلى طبيعة الشخص ولكن أسمحولي أن أقول أن النسبة الاكبر منا سوف تقوم بأضاعة الوقت ولن تنتهي من الدراسة والقراءة بشكل منتظم ولن تجبر نفسه على الدراسة إلا في أوقات الراحة ومن هنا تأتي فائدة وضع خطة عمل وانا أفضل دائما أن تكون الخطة بعيدة المدة يعني على الأقل سنة تضع فيه مخطط للكتب والشهادات التى يجب ان تنتهي منها في هذه الفترة أما الشرط الثاني الخاص بالتنظيم فهو لايقل شأننا عن الشرط الأول فبدون تنظيم لجدول حياتك اليومي خطتك لن تنجح وسوف تبدأ خطتك السنوية بالتغير تدريجا إلى أن تجد أن ميعاد أنتهاء المخطط الأول قد تغير وبالتالي تفقد خطتك المصداقية مع نفسك وتنساها وتبدأ بأعداد خطة جديدة تعود فيها إلى نقطة الصفر وكل هذا على حساب مستقبلك.

سألني أحد الأصدقاء سؤال في غاية البساطة كيف أنظم وقتي ؟ فقلت له أسأل نفسك كم ساعة في اليوم ؟فقال لي 24ساعة قلت له انت تنام سبع ساعات وتذهب إلى الجامعة ست ساعات وتضيع 3ساعات في الأكل والتلفاز ويبقى لك 8ساعات فهل لك ان تتخيل ماذا يمكن لك ان تفعله في هذه الثماني ساعات كم من الكتب تستطيع أن تقرأ وتتعلم ؟فأجابني أن هذا الكلام هو حبر على ورق وصعب تطبيقه في الحياة الواقعية ؟ قلت له إذا إقرا وأدرس ثلاث ساعات في اليوم وسوف تجد نفسك ومستقبلك بعد عام واحد قد تغير I80 درجة وإن لم يتغير سوف يتغير السنة القادمة وسوف تجد نفسك في تطور ملحوظ ومنظم وختمت معه بأن لو كان تفكيرك وعقلك الباطن مقتنع بأن الخطة هي كلام على ورق عندها سوف لن تكون انسان ناجح لان الأمر يحتاج إلى ارداة قوية وعزيمة أقوى لذا حدد موقف من الآن فأما نعم أو لا ؟

وأختم كلامي بحديث لرسولنا الكريم محمد صلى الله عليه وسلم "نعمتان مغبون فيهما كثير من الناس: الصحة والفراغ" لذا أعلم أخي العزيز أن الوقت الذي لديك يساوي ذهب لكن أحيانا نسيئ أستخدامه وتقديره وأعلم أيضا أن مهما كان عمرك أن هناك دائما متسع من الوقت تستطيع ان تحقق فيه أكثر بكثير مما تحلم به فترتفع أنت ونحن وأمتنا إلى مستوى أعلى وأفضل مما نحن عليه ولاتقل أبدا ان الوقت قد فات حتى لو كنت في الخمسين من العمر حاول أن تضع بصمتك في الحياة وحتى لو كانت هذه البصمة بسيطة.

أيمن النعيمي

المحررون الدائمون

- المهندس أيمن النعيمي
www.networkset.net
- المهندس عادل الحميدي
adel_husni2000@hotmail.com
- المهندس أحمد الشحات
warior10@hotmail.com
- المهندس ياسر رمزي
www.yasserauda.com
- المهندس عمر السويدي
om18899@gmail.com
- المهندس أحمد بخيت
www.abakhiet.info
- المهندس محمود عمر
mahmoudomr@gmail.com
- المهندس أحمد الجلجولي
ahm_ijal@hotmail.com

المحررون الضيوف

- المهندس أحمد مصطفى
www.amnetwork.blogspot.com
- المهندس محمد عبدون
www.learnbyvideo.maktoobblog.com
- المهندس محمد ناجى سيد
eng.mohamednagy@gmail.com
- المهندس اسلام محمود
islam.mahmoud@imholding.com
-
-

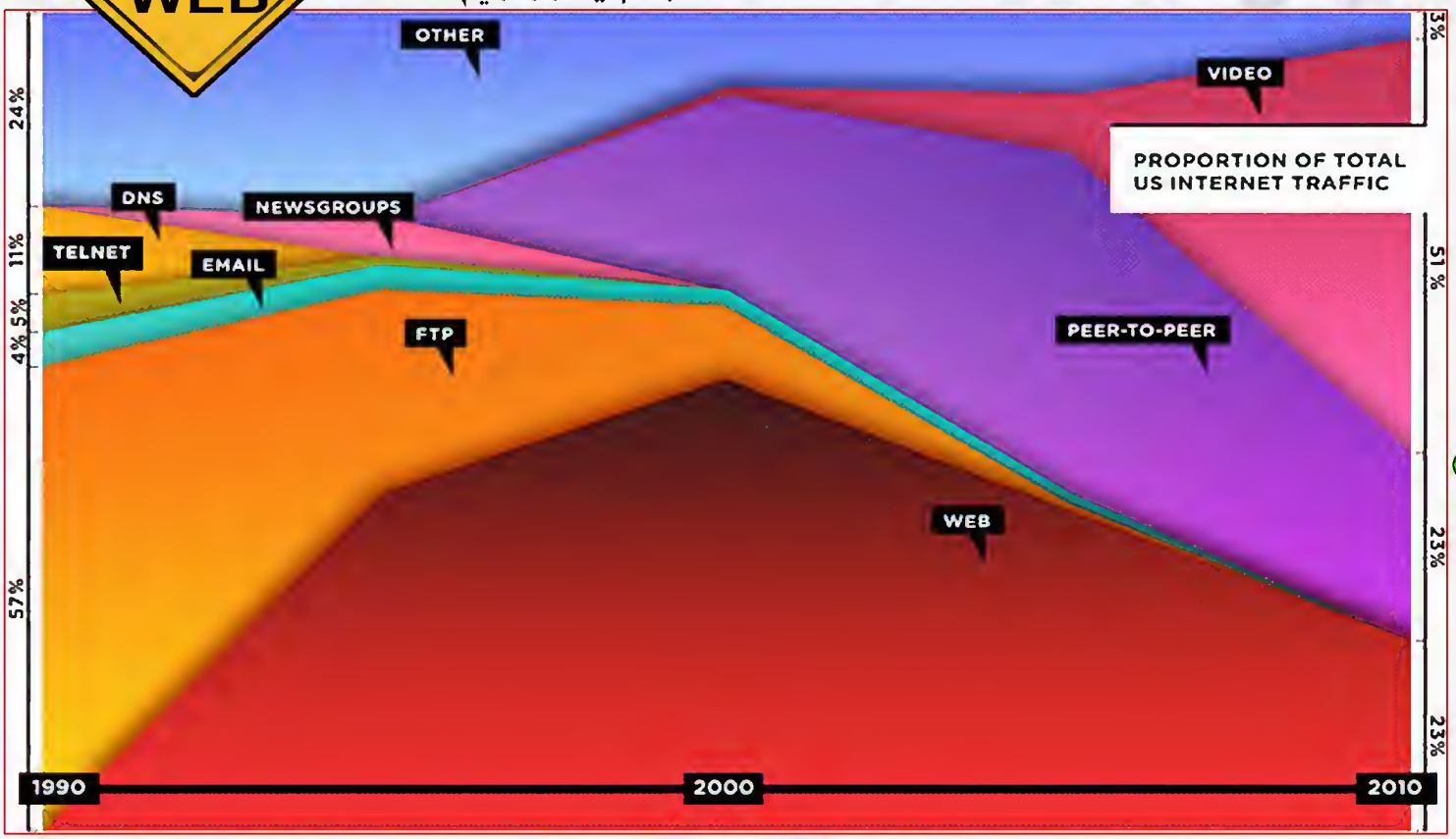
موقع المجلة
www.networkset.net
بريد المجلة
magazine@networkset.net
بريدي الخاص
admin@networkset.net

محتويات أكتوبر 2010

نهاية الويب

the END of WEB

بقلم: ياسر رمزي



خلال أشهر الصيف الماضيه دار نقاش في الاوساط العلميه بين الخبراء و على صفحات المجلات التقنيه المتخصصه في أمر هام و ننقل لكم بعض ما دار في النقاشات.

أصبح تصفح البريد الالكتروني و الدردشه الالكترونيه لدى البعض يتم عبر ال Iphone ,Ipad وباقي الهواتف الذكيه او ما نسميها ال Smartphones كالبلاك بيري و هي نفسها نستخدمها لسماع دفق من الموسيقى او مشاهدة دفق فيديو Video Streaming و استقبال ال RSS feeds وحتى بالمنزل تشاهد الافلام عبر خدمات كال love film streaming videos و نلعب الالعاب على xbox live

في الحقيقه نحن نقترب من نهاية الويب

الويب عمره الان 18عام (من عام 1992الي 2010) و لكن ما هو الويب ؟

الويب هو احد التطبيقات من عدت تطبيقات تستخدم شبكة الانترنت هذا التطبيق يستخدم بروتوكولات ال HTTP & HTTPS عبر المنفذ رقم 80و يرسل عبر بروتوكولات ال IP & TCP و محتوى هذا التطبيق بيانات مكوده عبر لغة HTML

أخر احصائيه هذا العام تقول ان اقل من ربع البيانات المستخدمه لشبكة الانترنت Internet Traffic هي بيانات ويب Web Traffic وهذة النسبة تتضائل كل يوم و من المتوقع ان تكون بنسبة لا تتجاوز ال 10% بعد خمس سنوات فعدد مستخدمي الانترنت عبر هواتفهم يزيد كل يوم عن عدد مستخدمي الانترنت عبر الحواسيب الشخصيه وفي تطبيقات بعيده بشكل او باخر عن الويب كبرامج التحدث الصوتي عبر بروتوكول الاي بي VOIP مثل ال Skype وبرامج الدردشه النصيه عبر البلاك بيري و هكذا

في عام 2010

23%من internet traffic هو web

23%من internet traffic هو peer to peer

51%من internet traffic هو video

3%من internet traffic هو others وهذا يشمل (DNS,FTP, NEWSGROUPS,EMAIL,TELNET)

الخبراء يقولون ان هذا امر طبيعي و لنا في الاختراعات القديمه عظه و اليكم بعض الامثله :

في 1920كان هناك في امريكا 186شركة خطوط حديده للقطارات و اليوم بقى فقط 7 شركات

في 1894اي اواخر القرن التاسع عشر بدأت شركة AT&T بالاستحواذ على الشركه الام لخدمة الهاتف و ظهرت معها 6000شركه مستقله و في 1939أمتلكت ال AT&T معظمها وأحتكرت ايضا سوق المكالمات البعيده بامريكا Long Distance Calls

في بداية 1900ظهرت المئات من شركات توفير الكهرباء و في نهايات القرن العشرين بقى منها بامريكا فقط 16شركه

يقول الخبراء ان هذة طبيعة مسار اي صناعه او اختراع جديد حيث يمر بمراحل معروفه هي

الاختراع Invention - الانتشار Propagation - الاعتماديه Control –Adoprion السيطره

المدافعين عن الويب يقولون ان الفرصه مازالت سانحه ليعود الويب او يبقى بنفس نسبة استخدامه الحاليه على الاقل وخاصة بعد ظهور الاصدار الخامس من HTML5الذي يوفر مرونه و طريق مفتوح للمحافظه على جودة الخدمه و أفق جديد لما يقدمه الويب لنا

والبعض في المعسكر الاخر يقول ان الويب سيبقى كمحتوى تجاري كمواقع الشركات و مواقع التعريف الشخصي و لكن ليس أكثر من ذلك

الانترنت اختراع بقيمه ثوريه كالكهرباء قابل للتطوير و بالتالي التغيير الشكلي اخيرا اخشى ان يأتي اليوم الذي نقول فيه

هل تتذكرون السنترلات الداخليه بالشركات من بانسونيك؟

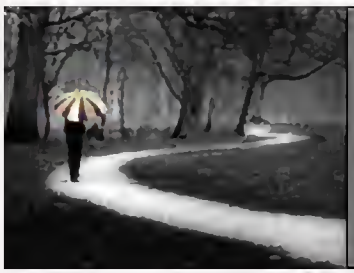
هل تتذكرون الفاكس

هل تتذكرون ال TV Cable

هل تتذكرون ال Netscape&ICQ

هل تتذكرون الويب؟؟؟

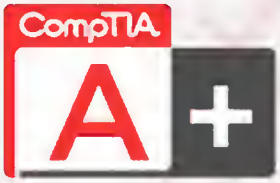
م.ياسر رمزي عوده مدير شركة CBTme.com بدولة الامارات العربيه المتحده



من أين أبدأ وكيف أبدأ في الشبكات ؟؟؟
سؤال لطالما حيرني !!!

بقلم: عادل الحميدي

حديثنا اليوم عن الشهادة الأولى في برنامجك لتصبح مهندس شبكات محترف خلال ثلاث سنوات ، والذي وضعناه سوياً لبناء مجد لأمتنا المسلمة المسلوب مجدها ، لذا جئتكم اليوم بمقدمة كتاب الدليل الدراسي الكامل للشهادة CompTIA A+ الإصدار الرابع)مع بعض التعديلات البسيطة(، ذلك الكتاب العربي الماتع والمعتمد من CompTIA ، والذي أنصح به المتدربين دائماً سواء يشتكون من اللغة الإنجليزية أم لا ...



ماذا تعني الشهادة A+ ؟

طوّرت CompTIA (Computer Technology Industry Association) أو (جمعية صناعة تقنيات الكمبيوتر) برنامج الشهادة A+ ليكون أداة مُعتَمدة للتحقق من كفاءة التقنيين المتخصصين في خدمة الكمبيوتر. تُمنَح هذه الشهادة لمن يصل بمعرفته ومهاراته إلى المستوى الذي يسمح له بتقديم دعم Support سليم في مجال الكمبيوترات الشخصية ، وهي تُشبه الشهادات الأخرى في مجال صناعة الكمبيوتر ، فشركة Novell مثلاً تمنح الشهادة CNE (Certified Novell Engineer) أو (مهندس معتمد من نوفل) ، وشركة مايكروسوفت تمنح الشهادة MCSE (Microsoft Certified Systems Engineer) أو (مهندس نُظم معتَمَد من مايكروسوفت) . فالفكرة وراء هذه الشهادات هي أنك حين تحتاج لأن ينفّذ أحدٌ خدمات تقنية على أحد منتجات هذه الشركات فإنك ستتصل فوراً بتقني يحمل شهادة في المجال المناسب للخدمة التي تريدها وليس بأول "خبير" تجده في دليل الهاتف .

لقد تم إنشاء برنامج الشهادة A+ لتقديم وخدمة نطاق واسع من الشهادات ، بمعنى أن الغاية منه هو تأكيد أن حاملها يتمتّع بخبرة في الكمبيوترات الشخصية صنع العديد من الصانعين/الباعة المختلفين . ولنيل الشهادة A+ يجب أن تنجح في إمتحانين هما :

1- الإمتحان الأول A+ Essentials (رقم 220-701)والذي يُغطي المفاهيم الأساسية للكمبيوتر ، واستكشاف وإصلاح الأجهزة ، وخدمة الزبائن ، وترقية الأجهزة والأمان والحماية .

2- الامتحان الثاني A+ Practical Application (رقم 220-702)والذي يُغطي كمية أكبر من النواحي العملية للمواضيع التي يركّز عليها الامتحان الأول Essentials .

قم بزيارة هذا الرابط :
http://www.comptia.org/certifications/listed/a.aspx

ملحوظة هامة : ليس بالضرورة أن تخضع للامتحان الأول Essentials والامتحان الثاني Practical Application في الوقت نفسه ، إذ يُسمح لك بـ 90يوماً كمهلة بين الامتحان الأول والثاني . لكنك لن تنال الشهادة A+ حتى تنجح في الإمتحانين .

ما الحاجة للشهادة A+ ؟

هناك عدة أسباب تستدعي الحصول على الشهادة A+ ، وقد وضعت CompTIA في اللوائح الخاصة بمعلومات المرشحين خمس مزايا أساسية :

- تُثبت مستواك الإحترافي في هذا المجال .
- تزيد من فرصك في إيجاد وظيفة .
- تفسح المجال أمامك للتقدُّم أكثر في مجالك المهني .
- بعض برامج التدريب المتقدمة أصبحت تضعها كشرط ضروري .
- تزيد ثقة الزبون بك وبخدماتك .

إثبات للمستوى الإحترافي :

أصبحت الشهادة A+ بسرعة من الرموز المميزة في مجال خدمات الكمبيوتر ، والشركات التي لديها موظفين يعملون في مجال خدمة الكمبيوتر تعرف تماماً فوائد هذه الشهادة وتدفع موظفيها للحصول عليها ، كما أن الكثيرين أصبحوا يعرفون أهمية وضع الشعار A+ Certified Technician أو (تقني حاصل على الشهادة A+) على بطاقات عملهم .

زيادة فرص العمل :

حاملو الشهادة A+ مُفضّلون عن غيرهم لدى أصحاب العمل ، كما أنهم مُرشّحون دائماً لنيل راتب أكبر لأنهم يوفرون على أصحاب العمل المصاريف التي يتطلبها تدريب الموظفين على كل تقنية جديدة يريدون استخدامها .

فرصة أكبر للتقدّم :

معظم العلاوات والترقيات تُمنَح بحسب الأداء ، والتقنيون حاملو الشهادة A+ يعملون بسرعة وكفاءة أكبر مما يزيد من إنتاجيتهم في العمل . كلما كان الموظف منتجاً أكثر كلما حقق دخلاً أكبر للشركة ، وطبعاً كلما حقق الموظف دخلاً أكبر للشركة كلما كانت مكانته فيها أكبر . لذا فإن نيل هذه الشهادة يزيد الفرصة في التقدُّم على سُلّم الترقية

تحقيق متطلبات التدريب :

الشهادة A+ مُعتَمدة لدى كثير من شركات الكمبيوتر الرئيسية . وبعض تلك الشركات تضع الشهادة A+ كأحد المتطلبات المسبقة لبرامج الشهادات الخاصة بها كشهادات مايكروسوفت وسيسكو ، فإنك ستجد في تلك الكورسات دائماً ما ينصح بأن يكون المتدرب حاصل على شهادتي N+,A+ كمتطلب سابق ، وبذلك تنخفض تكاليف تدريب الموظفين .

زيادة ثقة الزبائن :

على اعتبار أن الشهادة A+ أصبحت معروفة جيداً بين أصحاب الكمبيوترات فإن الكثير منهم أصبح يعرف أن حامل الشهادة A+ مؤهّل أكثر من غيره للعمل على معدات كمبيوتره الخاص .

كيفية الحصول على الشهادة A+ :

يمكن لأي شخص أن يحصل على الشهادة A+ بمجرد نجاحه في الإمتحانين ، وليس بالضرورة أن يعمل لدى شركة معينة . إنها ليست جماعة سرية ، وإنما مجموعة من النخبة . للحصول على الشهادة A+ عليك القيام بما يلي :

- اجتياز الامتحان A+ Essentials (رقم 220-701).
-2اجتياز الامتحان A+ Practical Application (رقم 220-702).

ملحوظة : إذا كنت تحمل الشهادة A+ من قبل)الامتحانات رقم : 220-601، 220-602، 220-603، 220-604)تسمح لك CompTIA بالخضوع لأحد الامتحانات من أجل ترقية شهادتك ، فهذه الشهادات انتهت منذ فترة وجيزة قرابة الشهر وأصبحت كما يقولون Expire منتهية الصلاحية ، حيث حدث تقدم كبير في مجال الكمبيوترات في السنوات الأخيرة ما تطلب معه تغير المناهج الخاصة بـ A+ . يمكنك التقدُّم للإمتحانات لدى أي مركز اختبار تابع لـ Thompson Prometric أو Pearson VUE . إذا اجتزت الامتحانين بنجاح ستحصل على شهادة من CompTIA بالبريد تقول أنك نجحت . وستسلم أيضاً مشبكاً

للصدر وبطاقة عمل .

أو يمكنك التقدّم للامتحانات والتسجيل عن طريق الإنترنت من خلال موقع
Prometric : http://www.prometric.com/default.htm
VUE : http://www.vue.com/

وعندها ستكون التكلفة أقل ، وسيطلب منك للتسجيل والإمتحان اسمك ، وعنوان البريد الإلكتروني الخاص بك ، ورقم هاتفك ، والشركة التي تعمل بها ، وموقعك الجغرافي ، وأين (المركز التابع لهم) ومتى تريد الخضوع للإمتحان ، ورقم الفيزا كارد (يجب الدفع أثناء التسجيل) .

ملحوظة : لا توجد خصومات أكثر من ذلك ، وإذا احتجت إلى الخضوع لنفس الإمتحان مرة ثانية فعليك أن تدفع كامل المبلغ في المرتين . وأحيانا يكون هناك ما يسمى بالفوتشر والذي يعني أنه يحق لك إعادة الإختبار مجاناً .

معلومات إضافية : ما هو الترخيص ASC ؟

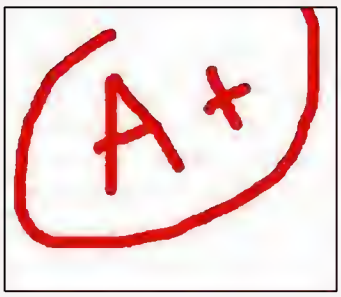
يزداد عدد شركات الخدمة التي تسعى للحصول على الترخيص ASC (Authorized Service Center) أو (مركز خدمة A+ مُعتَمد) ، وهذا الترخيص يعني أن أكثر من خمسين بالمئة من موظفي الشركة يحملون الشهادة A+ . يعرف الزبائن والباعة على حد سواء أن مراكز الخدمة الحاصلة على هذا الترخيص توظّف التقنيين المتخصصين والأكثر كفاءة ، ولهذا نجد أن هذه المراكز تحصل على أعمال أكثر بكثير من المراكز غير المُرخصة . وبما أن الكثير من مراكز الخدمة تسعى للوصول إلى المستوى ASC فهذا يعني أنها تُفضّل توظيف حاملي الشهادة A+ على غيرهم .

المواضيع المطلوبة للإمتحان :

مع كل إمتحان يتعلق بأحد مجالات الكمبيوتر لابد من وجود مواضيع مطلوبة فيه ، وهي المواضيع التي يرغب القائمون على الإمتحان بإختبار كفاءتك فيها . كما ذكرنا سابقاً ، تحتاج لنيل الشهادة A+ لخوض إمتحانين وهنا سنسرد المجالات التي يجب أن تبرع فيها كي تجتاز كلا الإمتحانين الرسميين .

ملحوظة : من الوارد في أي وقت أن تتغير المواضيع المطلوبة في الامتحان دون أي إنذار مسبق من CompTIA . لذا إذا أردت التأكد من القائمة الأخيرة للمواضيع المطلوبة يمكنك زيارة الصفحة الخاصة بالشهادة A+ في موقع CompTIA .

ما يلي هي النواحي (أو الميادين ، وفقاً لمصطلحات CompTIA) التي يجب أن تكون خبيراً فيها من أجل النجاح في الإمتحانين الخاصين بالشهادة A+ :



الميدان الأول : مكوّنات الكمبيوتر الشخصي (التثبيت والتكوين والترقية) .
الميدان الثاني : الكمبيوترات المحمولة والأجهزة المحمولة .
الميدان الثالث : أنظمة التشغيل (الماك والويندوز واللينوكس) .
الميدان الرابع : الطابعات والماسحات .
الميدان الخامس : الشبكات .
الميدان السادس : الأمن والأمان .
الميدان السابع : مسائل السلامة والبيئة .
الميدان الثامن : الإتصال والإحترافية .

وهذه بعض النصائح من CompTIA : أرجو قراءتها (هامة جداً وفيها تفاصيل مثيرة)
http://www.comptia.org/certifications/testprep.aspx
http://www.comptia.org/certifications/testprep/trainingmaterials.aspx

نصائح هامة حول طريقة إدارة وتحليل الشبكات

بقلم: عمر السويدي

وصلتني بعض رسائل من إخوة منهم من يشكر ومنهم من يستفسر، وجزا الله تعالى الجميع على تواصلهم، وأرجو لهم الازدياد. لذلك سوف أخصص هذه المقالة لكي أتحدث عن طريقة إدارة تخصص تحليل الشبكات على شكل نقاط ونصائح هامة ، وذلك كون هذا التخصص مازال يعتبر مفهوم جديد وغير منتشر في عالمنا العربي، وكذلك لما له من تداخل مع التخصصات الأخرى ، مثل البرمجة وإدارة الخوادم ومركز المعلومات والـ SLAs وغيرها.

لا بد من أنك قد علمت الآن أن التوصل إلى مصدر المشكلة قد يكون عائقاً لا بد لك من اجتيازه، فهو يتطلب جهدا وعملا.

فأحيانا تمر عليك مشكلة تحار فيها أشد الحيرة، حول مكانها، أو على الأقل كيف تبدأ بعملية تحليل المشكلة حتى يظهر لك محلها لكي تقوم بحلها. أحياناً تجد أن المشكلة ليست في الشبكة بل هي في جهاز معين مرتبط بالشبكة، لكنك لا تستطيع أن تثبت ذلك حتى يتم التعامل مع المشكلة. أحياناً تخشى أن يساء فهمك وأنك تحاول التخلص من هذه المشكلة برميها نحو زميلك في العمل.

هناك الكثير والكثير من الأسباب الأخرى التي يمكن ذكرها.

أعود فأقول حتى تتجنب هذا النوع من المشاكل لا بد لك من نقاط مهمة:

1- معرفة وإلمام بالـ protocols لأنها وظيفتك ويجب أن تعلم كيفية عمل هذه البروتوكولات.

2- يجب أن يكون كلامك دائماً موثقاً، كالطبيب، فالطبيب لا يستطيع أن يقول الاحتمالات جزافاً، لأن حياة الناس ليست لعبة. كذلك عملهم وأوقاتهم يجب أن نحترمها.

3- لا تكن ذا نظرة سلبية، فأنت لو أتى أحد وأشار إلى عطل في الشبكة وهو لم يفحصها، لثرت في وجهه وغضبت عليه، كذلك الناس بالكلام الطيب اللين وبالإفهام، قد يتقبلون. (أعني قد يتقبلون وليس أكيداً)

4- عندما تشير إلى موضع الإشكال، يجب أن تكون متأكداً بنسبة 99% وإلا تأثر عملك مستقبلاً وصرت غير موثوق، وعندما تحدث مشكلة سوف يقومون بلومك وكذلك فهم لن يصدقوك عندما تخبرهم عن مكان المشكلة.

لا أحاول إخافتك من هذا التخصص، لكن لمدى تأثيره أحاول أن أعطيك صورته

الحقيقية. فهو مهم من الناحية الأمنية، ومهم من الناحية المادية (هل تعلم كم ستوفر من الأموال على شركتك؟! وهل تعلم بهذا الفعل كيف ستكون إنساناً محبوباً!!)

أعود فأقول، إدارة هذا التخصص وماذا أعني بها.
هذا التخصص ليس مرتبط بشركة معينة، فهو ليس على ارتباط بشركة Cisco أو شركة Juniper أو شركة Oracle أو أي شركة أخرى.
بل هو قائم بذاته ومرتبط ارتباطاً وثيقاً وكلي بخطوط الاتصال وبال protocols. الرابط بينك وبين الشركات التي ذكرتها وغيرها هو ال protocols وأسلاك الشبكة، وكيفية عمل تلك الأجهزة.
وبالمثال يتضح المقال:
سرعة الاستجابة بين نقطة (أ) ونقطة (ب) يجب أن تكون 9 milliseconds إلى 20 milliseconds مثلاً، بغض النظر ماذا موجود في المنتصف من أجهزة ربط شبكي switches.
فعندما ترتفع إلى 40 milliseconds فهذا يعني بداية ما قد يكون مشكلة لك في المستقبل.
بمثالنا الذي ذكرناه، كما ترى لم نهتم ما هي الأسلاك المستخدمة أو ما هي الأجهزة، لكني أعلم مسبقاً أن السرعة يجب أن تكون هذه لأنني كنت قد فحصتها مسبقاً عندما كنت أعمل وثائق الاتصال التأسيسية base lining، فعلمت أن السرعة في الوقت الطبيعي 9أجزاء من الثانية وقد ترتفع إلى 25جزء من الثانية، وإن زادت زيادة ليست بالقليلة كعشر أجزاء من الثانية مثلاً، أعلم أن هذا لا بد أن يثير انتباهي.

الشيء الآخر في إدارة هذا التخصص هو أن أنشر المعرفة به، بمعنى أتواصل مع الزملاء في العمل فأخبرهم بين فترة وأخرى عن كيفية العمل في هذا التخصص حتى تكون لديهم معرفة نوعاً ما فلا يستغربون مني الأسئلة التي أطرحها عليهم عندما أحاول حل مشكلة ما.

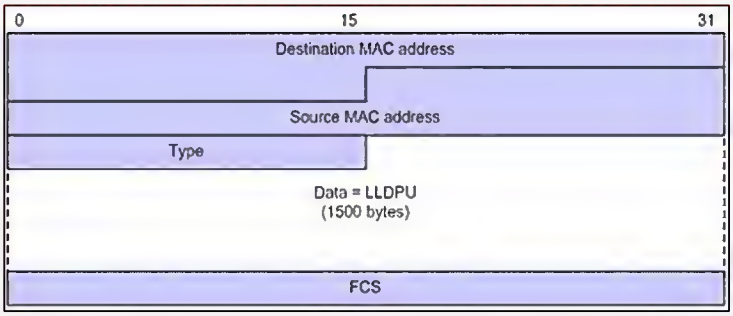
كذلك لا بد لي من معرفة شيء مهم، التوثيق، التوثيق، لا بد منه. لأنه كما قلت وكما سأستمر في القول ما قد يكون بطئاً عندي، قد لا يكون كذلك عندك، فالأمر هنا نسبي، فإن لم توثق وتقل لي كانت سرعة الاستجابة هكذا وارتفعت إلى كذا، فلن أتوقع أن هذا الأمر غير طبيعي.
لا بد من الأرقام ولا بد من التوثيق.
لا تستعمل في التوثيق، السرعة جيدة اليوم، السرعة جيدة جداً اليوم... إلخ. فلن تفيد شيئاً، بل اذكر الأرقام وفي خانة أخرى اكتب هل هذا الرقم يعني جيد أو جيد جداً أو مقبول، وهكذا. أو افعل كما يفعل البعض يستخدم التعابير فعندما يستخدم وجهاً مبتسماً أخضراً يعني كل شي تمام، ووجهاً أصفر يعني بدأنا في مرحلة الخطأ.

بروتوكول الـ LLDP بديل الـ Cisco Discovery Protocol

بقلم: أيمن النعيمي

بداية وقبل كل شيء يجب أن نعطي للعالم حقوقها فهذا البروتكول أو فكرة هذا البروتوكول كان من أنتاج وتطوير مركز أبحاث سيسكو ومنذ زمن طويل يعود إلى عام 1994وسمي حينها بي CDP أو Cisco Discovery Protocol لذا فوجود بروتوكول الـ LLDP أو Link Layer Discovery Protocol يعود فضله إلى سيسكو أولا وخصوصا لو قلت لك أن عملية تطوير هذا البروتوكول تمت بالتعاون بين شركة سيسكو ومنظمة الـ IEEE عام 2000وبعد خمس سنوات من العمل على هذا البروتوكول وفي عام 2005ظهر لنا هذا البروتوكول وأعتمد رسميا وحصل على الكود 802.1AB وتحت أسم LLDP-MED أو LLDP-Media Endpoint Discovery والذي كان نسخة مطورة من الـ LLDP العادي كونه يعطي معلومات أكثر وأدق مثل معلومات حول الفي لان ودعم لـ VOIP والـ PoE وحالة الـ Duplex والخ....

فكرة عمل هذا البروتوكول بسيطة جدا وتعتمد بالمقام الأول على الـ MIB والتي تحدثت عنها في عدد سابق من المجلة حول بروتوكول الـ SNMP , الـ MIB أو Management Information Base هي قاعدة بيانات وهمية خاصة ببروتوكول الـ SNMP ففيها يتم تجميع المعلومات وأرسالها إلى الجهاز الذي يقوم بتحليل ومراقبة الجهاز ومن هذه الفكرة البسيطة ولدت فكرة هذا البروتوكول فلو عدنا قليلا إلى موضوع الـ SNMP لوجدنا أن هناك مايسمى بي الـ Agent والذي يكون موجود على الروتر او السويتش وهو من يقوم بأرسال المعلومات إلى مركز تحليل البيانات معتمدا على الـ MIB كمصدر معلومات ومن هنا فكر مطوري هذا البروتوكول لماذا لايكون هناك Agent يقوم بأرسال وتبادل بعض المعلومات لكن بين الأجهزة وفقط وبشكل بسيط وغير معقد جدا كما في بروتوكول الـ SNMP وكل هذه العمليات تتم بين الاجهزة من خلال Multicast Address مثلها مثل بروتوكول الـ CDP والذي يعتمد على العنوان الآتي 01-00-0c-cc-cc-cc في أرسال واستلام المعلومات بين الأجهزة بينما يستخدم الـ LLDP العنوان التالي 01-80-c2-00-00-0e وأحب أن أشير من هنا إلى نقطة مهمة وهي تقول أن بروتوكول الـ LLDP هو one way protocol وبكلام آخر المعلومات التي ترسل لايسمح لها بان تمر من خلال أكثر من جهاز أي انها تصل إلى الجهاز التالي وتتوقف لذا نجد هذه البروتوكولات تعطينا معلومات بالجيران المحيطة بنا فقط .
يقوم الـ LLDP بأرسال المعلومات على شكل فريم وتكون محتوياته على الشكل التالي



الحقل الأول والثاني مفهومان الحقل الثالث الخاص بي الـ Type يتم كتابة كود الأيثرنت 0x88CC كون أغلب الكابلات تعتمد على الأيثرنت الحقل الرابع وهو الحقل الأهم والذي توضع فيه المعلومات LLDP Data Unit أما الحقل الآخير فهو معروف أيضا ومعناه Frame check sequence وهو من أجل التأكد من صحة وصول المعلومات .
وآخيرا أحب أن أختم مع هذا الجدول الهام والذي حصلت عليه من موقع سيسكو وفيه توضيح لأهم الأختلافات بين بروتوكول سيسكو CDP وبروتوكول الـ LLDP

Protocol Operation	LLDP	Cisco Discovery Protocol
Use of multicast address	Yes 01-80-C2-00-00-0E	Yes 0100.0ccc.cccc
Ethertype	LLDP has a dedicated ethertype: 88-CC.	Cisco Discovery Protocol uses IEEE 802.2 and 802.3 encapsulation only.
Token Ring support	Yes	Yes
Fiber Distributed	Yes	Yes
Ethernet support	Yes	Yes
ATM support	No (not formalized)	Yes
Frame Relay support	No (not formalized)	Yes
Checksum support	No	Yes
Fast Start support	Yes	Yes
MIB support	LLDP-EXT-MED-MIB	CISCO-CDP-MIB
Topology change notification	Yes	Yes
Standard 802.1x interaction	The switch does not accept or send LLDP-MED packets until after authentication occurs.	The switch does not accept or send Cisco Discovery Protocol packets until after authentication occurs.
Advertising frequency (time between protocol frames)	Default 30 seconds (configurable)	Default 60 seconds (configurable)
Transmit frame on local MIB change-If one of the settings in the local MIB changes	Yes	No
Third-party device action on receiving an LLDP-MED or Cisco Discovery Protocol	Accept, depending on their support for LLD-MED and configuration	Most switches ignore the Cisco Discovery Protocol messages but forward them.
Discovers Cisco devices	Yes	Yes
Discovers third-party devices	Yes	No

GNS3 Memory Usage Optimizations

بقلم: احمد مصطفى

```
model = 3660
ghostios = true
sparsemem = true
 [localhost]
     [[3660]]
    image = \Program Files\Dynamips\images\c3660-ik9o3s-mz.
124-10.image
     [[router r1]]
      fa0/0 = sw 1      # Note that you can use two letter interfaces
names
                  # for increased clarity if you wish
     [[router r2]]
     fa1/0 = sw 2
     [[router r3]]
     fa1/0 = sw 3
     [[ETHSW sw1]]
1 = access 5
OMITTED
```

- يمكن وضعها تحت كل نوع من أنواع الراوترات علي حدي، وذلك إذا كان عندنا أكثر من نوع في الـLAB فمثلاً:

```
autostart = False
[localhost:7200]
  workingdir = EXAMPLE.working
  udp = 10000
  [[3725]]
        image = C:\Documents and Settings\Administrator\My
Documents\ios\c3725-adventerprisek9-mz.124-15.T5.bin
    ram = 128
    ghostios = True
    idlepc = 0x60bedba0
  [[7200]]
        image = C:\Documents and Settings\Administrator\My
Documents\ios\C7200-AD.BIN
    idlepc = 0x8046b800
    ghostios = True
  [[3640]]
        image = C:\Documents and Settings\Administrator\My
Documents\ios\C3640-IK.BIN
    idlepc = 0x60618538
    ghostios = True
    chassis = 3640
OMITTED
```

-3لا يمكن وضع الـghost ios في موضعين:

أ- router level: فمثلاً المثال السابق تم اختصاره، ولكن لو أكملنا بقية الـ con-figuration نجد التالي:

```
[[ROUTER R1]]
      model = 3640
      console = 2000
      slot0 = NM-1FE-TX
      f0/0 = R3 f0/0
      slot1 = NM-1FE-TX
      f1/0 = R2 f0/1
   [[ROUTER R2]]
      model = 3725
      console = 2001
      f0/0 = R3 f1/0
      f0/1 = R1 f1/0
    [[ROUTER R3]]
      console = 2002
      f0/0 = R1 f0/0
      slot1 = PA-FE-TX
      f1/0 = R2 f0/0
[GNS3-DATA]
   configs = EXAMPLE_configs
   workdir = EXAMPLE_working
```

كثير منا حينما استخدم البرنامج Gns3 لأول مرة لاحظ البطء الشديد في الجهاز ثم بعد ذلك لما تعرف علي معلومة الـ Idle Pc لاحظ الفرق الكبير في معدل استخدام البروسيور حتي إنك تستطيع تشغيل اكثر من عشر راوترات في نفس الوقت دون أن يستهلك ذلك نسبة كبيرة من البروسيسور، فما السبب في ذلك؟

نقول مستعينين بالله سبحانه وتعالي:

يعتمد البرنامج علي وسيلتين لتقليل نسبة استخدام الذاكرة الحقيقية Real Memory ونسبة الذاكرة الوهمية Virtual Memory التي يستخدمها البرنامج وهما:

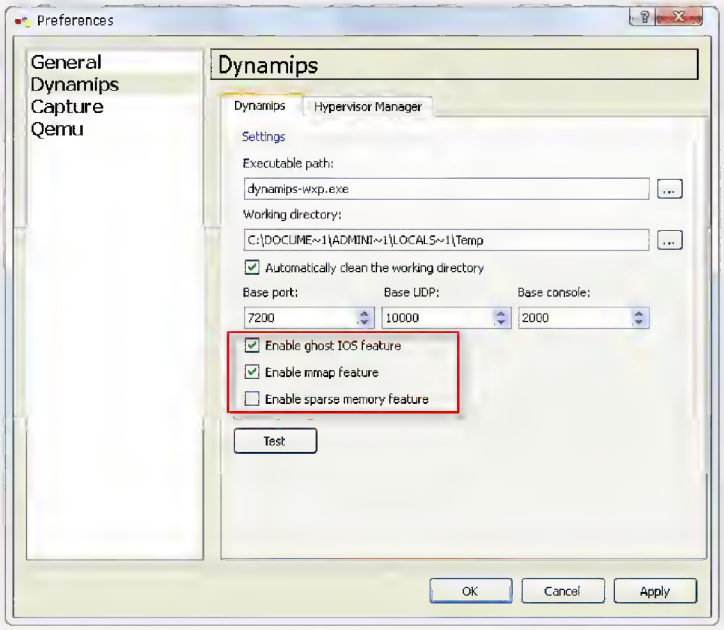
ghost ios

حينما تقوم بتشغيل عدة راوترات من نفس النوع ولنقل مثلا 3640-وهي أخف نسخة علي الجهاز-، فبدلا من أن يقوم كل راوتر علي حدي بتخزين نسخة من الـ IOS المستخدمة في الـ virtual RAM الخاصة به، وبالتالي مع زيادة عدد الراوترات تزيد نسبة الـvirtual RAM المستخدمة بصورة كبيرة- يقوم البرنامج بعمل shared memory لجميع الراوترات المستخدمة في اللاب بشرط أن تكون جميع الراوترات من نفس النوع.

فمثلاً إذا كان عندنا 10راوترات من نفس النوع وحجم كل واحدة 50ميجابايت، هنا نلاحظ أننا نحتاج إلي 500ميجابايت من Real RAM لهذه الراوترات مح ملاحظ بطء شديد في الجهاز عند محاولة تشغيل العشرة راوترات في نفس الوقت، ولكن مع خاصية الـ ghost ios، يقوم البرنامج باستخدم 50ميجابايت فقط من الـReal RAM لأنه يستخدم نفس نسخة الـIOS لجميع الراوترات المستخدمة.

كيف يتم تفعيل هذه الخاصية؟

هذه الخاصية مفعلة في برنامج الـGNS3 وذلك By Default ونلاحظ ذلك كما في الصورة التالية:



ولكن نلاحظ أن هذه الخاصية غير مفعلة في الوضع الإفتراضي Defualt في برنامج الـDynagen،والسبب في ذلك أنك تقوم بكتابة جميع الجمل في ملف الـ"net."، لذلك نقوم بتفعيلها باستخدام الجملة التالية

```
ghostios = true
```

ولكن السؤال هنا، أين نضع هذه الجملة؟

هل نضعها في أول ملف الـ"net." أم نضعها تحت كل راوتر علي حدي؟

حقيقةً أن هذه الجملة يمكن وضعها في عدة أماكن:

1- يمكن وضعها في بداية ملف الـ"net." وهذا يسمي top level parameters، وهنا يتم تطبيق هذه الخاصية علي جميع الراوترات الموجودة في الـLAB وذلك كما في المثال التالي:

ونلاحظ أن هذا المستوي لا يمكن وضع قيمة الـghost ios فيه، وهذا ينطبق أيضاً علي جميع المعلومات التي يتم وضعها في بداية ملف الـ"net." أو ما يسمي top level parameters، وإذا تم وضعها في هذا المستوي يتم تجاهلها.

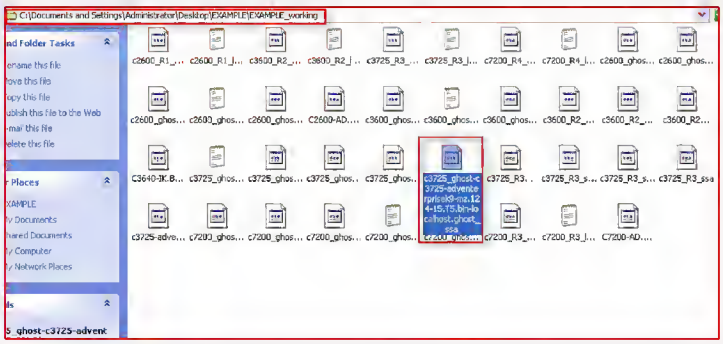
ب- server level:

كما في المثال التالي:

```
# Working with multiple dynamips servers
# A windows server (the local machine)
[xplt]

  [[7200]]
    image = \Program Files\Dynamips\images\c7200-ik9o3s-mz.
122-15.T17.image
    ram = 96

  [[ROUTER R1]]
    # Connect to s1/0 on R2 running on a different server
    s1/0 = R2 s1/0

# A linux server
[bender]
workingdir = /home/greg/labs/dist1
  [[7200]]
    image = /opt/7200-images/c7200-ik9o3s-mz.122-15.T17.image
    ram = 96
```

ماذا يحدث بعد تحديد هذه القيمة؟

بعد تحديد هذه القيمة يتم وضع ملفات امتدادها .image.ghost في نفس المسار الذي يتم وضع ملفات الـnvram فيه، وذلك لكل نوع من أنواع الراوترات في الـLAB، ما في الصورة التالية:



وهذ الخاصية تسمي MMAP، وهي المشار إليها في الصورة الأولي، وهذا الملف يمثل الـ shared memory region

sparemem

وهي الخاصية الثانية التي يعتمد عليها البرنامج في تقليل نسبة استخدام الذاكرة الوهمية Virtual Memory.

تقوم أنظمة التشغيل بتحديد نسبة معينة من الـVirtual Memory لكل process، فمثلاً في أنظمة الويندوز كل process لها 2جيجابايت من الـ Virtual Memory كحد أقصي، وفي أنظمة اللينوكس كل process لها 3 جيجابايت من الـVirtual Memoryكحد أقصي، وذلك في الأنظمة التي تعمل 32-bit.

هذا الحد يسمح لك بتشغيل 4راوترات علي أنظمة ويندوز، كل راوتر يستخدم 256ميجابايت من الـVirtual Memory، أما باقي الـ 2جيجابايت فهي تستخدم مع باقي العمليات التي يقوم بها البرنامج مثل :

- VM space used by cygwin
- libraries used by dynamips
- scratch space

هنا تقوم خاصية الـ sparemem بتخصيص الـVirtual Memory للراوتر الذي تستخدمه الـIOS فعلياً في الوقت الحالي وذلك لكل نوع من أنواع الراوترات المستخدمة، فمثلاً إذا كان الـLAB يحتوي علي أكثر من INSTANCE هنا يتم تفعيل هذه الخاصية لكل INSTANCE علي حدي.

لذلك فمن المستحسن عند تطبيق أي LAB أن تكون جميع الراوترات المستخدمة من نفس النوع.

كيف يتم تفعيل هذه الخاصية؟

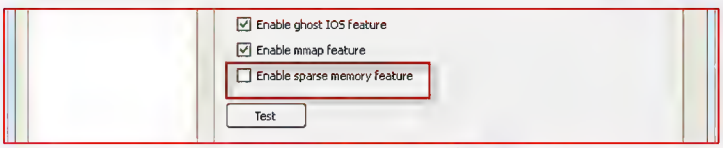
هذه الخاصية غير مفعلة By Defualt في الـGNS3 والـDYNAMIPS يتم تفعليهما كالتالي:

1-DYNAMIPS:

وذلك في الـTop Level Parameters عن طريق الجملة التالية:

```
model = 3660
ghostios = true
sparsemem = true
```

2- GNS3:



وفي الختام أسأل الله عز وجل أن ينفكعم بهذا العلم

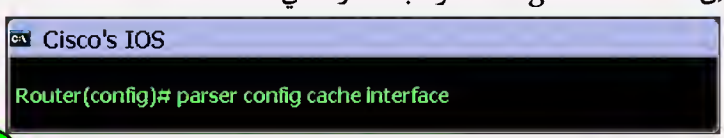
ولا تنسوني من صالح الدعاء

كيف تقوم بأظهار الأعدادت على أجهزة سيسكو بثواني

بقلم: أيمن النعيمي

مع كثرة الاوامر التى أشاهدها وأتعلمها كل يوم لازلت أجد نفسي لا أعرف شيء عن نظام سيسكو IOS فاليوم وأثناء جولاتي التى لاتتوقف على الأنترنت وجدت أمرا مفيدا ومهما ووظيفته تسريع ظهور الأعدادات الموجودة على الروتر وخلال 3 ثواني بس تظهر لك كل الأعدادات الموجودة على الـ Run-config

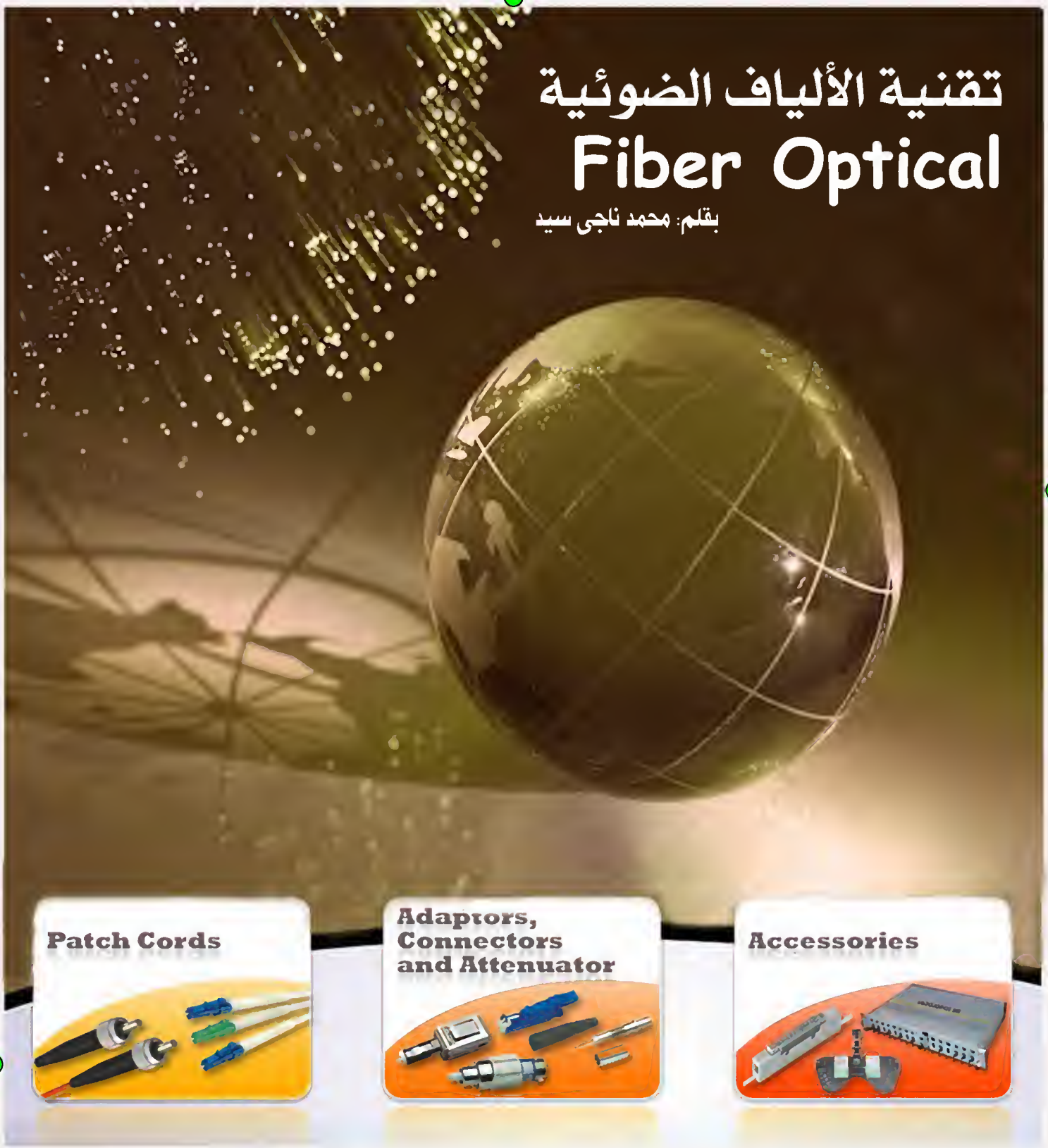
وقبل أن اذكر لكم الامر أحب أن أبين لكم فكرته فهو ببساطة يقوم بعمل Casheing للأوامر الخاصة بالمنافذ ويساعدك بشكل أسرع لأظهار النتائج وقد قمت بتجربة صغيرة لكي أحدد هل هناك فرق بالفعل في اظهار النتائج أم لا وفي التجربة التى قمت بها على الداينامبس قمت بأضافة روتر وركبت عليه 20منفذ سيريال وإيثرنت وقمت بتشغيل الروتر وتنفيذ الأمر Show run وكانت النتيجة أني انتظر حوالي الخمسة عشر ثانية حتى تظهر النتائج وبعدها توجهت إلى الـ Configure Mode وكتبت الأمر التالي



وعدت مرة ثانية ونفذت الأمر Show run والنتيجة أنني أنتظرت نفس الوقت وهو 15ثانية لكن في المرة الثالثة وبعدما تم عمل cache للأعدادات ظهرت النتائج خلال 3ثواني فقط وكله بفضل الأمر السابق والذي كما ذكرت في البداية بانه يقوم بعمل cache للأعدادت الخاصة بالمنافذ وأظهارها بشكل أسرع وبالتالي رفعنا قليلا من أداء الروتر وخصوصا أن هناك روترات قد تستغرق أكثر من دقيقة حتى تظهر النتائج وهذه الخاصية تم اضافتها أول مرة في النسخة 12.2وأصبحت جزء من النظام اعتبارا من النسخة 12.3وآخيرا هل تتفق معي أننا مازلنا جاهلين للكثير من أوامر سيسكو أم أنني الوحيد الذي لايعرف هذه الميزة ؟

تقنية الألياف الضوئية
Fiber Optical

بقلم: محمد ناجى سيد



تعتبر الألياف الضوئية أكثر التطورات الحديثة في أنظمة الاتصالات حيث كانت الكوابل النحاسية هي العنصر الأساسي في أنظمة الاتصالات و كان الموصل المعدني هو الوسط الذي كانت تنتقل المعلومات من خلاله في صورة أشارات كهربيه.الآن تم تعويض الوسط التراسلى بألياف ضوئية حيث تنتقل المعلومات خلال شعيرات زجاجية محملة بإشارات ضوئية. يعود تاريخ استخدام الضوء في نقل المعلومات إلى عام 1934عندما تم تسجيل اول اختراع لنظام اتصال ضوئى وذلك عندما بدأ الإنسان يؤول ما يراه بعينيه. ظهرت أشكال مختلفة من التواصل البصري بدءاً من إشارات الدخان التي ابتدعها الهنود الحمر في القرن الرابع قبل الميلاد. في القرن الثاني قبل الميلاد كان هناك نظام الإشارات الضوئية علي منائر البحر الأبيض المتوسط الذي وضعه الإغريق واستخدمه الملاحون لإرشادهم وتوجيههم أثناء رحلاتهم البحرية ويعتبر أول نظام تراسل باستخدام الشفرات الضوئية. وكانت هذه الأنظمة محدودة المدى ،إذ لم تكن تتعدى مدى البصر كما كانت محدودة النطاق إذ لم يكن بالإمكان إرسال أكثر من معلومة واحدة

أهم التطورات الأساسية في مجال الألياف الضوئية

1934 تسجيل اختراع أول نظام اتصال ضوئي .
1958 جائزة نوبل لاختراع الليزر .
1962 أول صمام ليزر من أشباه الموصلات .
1966 اكتشاف تشالزكاو لاستخدام شعيرات الألياف الزجاجية لانتقال الأشعة الضوئية.
1975 وضع الاتصال الضوئي في مجال الاختبار.
1978 أول إنتاج لأجهزة لحام الشعيرات الضوئية بالانصهار .
1982 بداية عصر الألياف الضوئية في أنظمة الاتصالات .
1984 بداية استخدام الألياف الضوئية في اتصالات بعيدة المدى في السويد .
1990 تم إنشاء أول شبكة ألياف ضوئية تربط بين شرق وغرب أوربا
1992 وضع شبكة الألياف الضوئية في خدمة المشترك في مجال الاختبار .
2000 استخدام الألياف الضوئية في أحدث أنظمة الاتصالات الدولية

ومع دخول انظمة الفايبر الى عالمنا العربى بقوة والتى مع السنوات القليلة القادمة ستكون هى مركز اى شبكة سواء كانت شبكات الاتصالات او شبكات النتورك وذلك لتوفير العديد من الخدمات مثل
(VoIP, high definition television (HDTV), videoconference, adsl, video telephony, E- BANK , E-BOOK , online –education , online-shopping)..etc

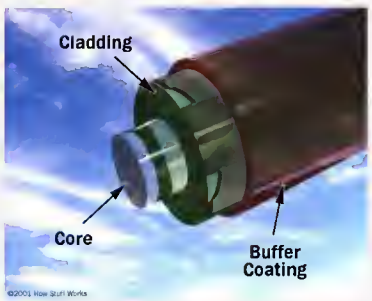
ولما لذلك اهمية فى مجال الشبكات حيث لايوجد شبكة الان الا وبها فايبر اوبتك للربط بين ال core switches او ال core switch and distribution فسوف نتعرف فى هذا المقال على انظمة الفايبر اوبتك

اولا مميزات الفايبر اوبتك

- لا تتأثر بالمجال الكهربي أو المجال المغناطيسي . Freedom electromagnetic field
- خالي تماماً من التداخلات (for Freedom) Cross talk
- قلة تأثره بالمياة . Low effect for water
- صعوبة التصنت عليه . High security
- تناسبها لنقل إحمال عالية على الشبكة . Traffic High (BW)
- قلة الفقد وخاصة في المسافات البعيدة . loss Low Transmit ion
- قلة معدلات تعطلها . Low fault rate
- خفيف الوزن . Low weight
- اقتصادي التكاليف . Economic

ماهى الالياف الضوئية

الألياف الضوئية هي ألياف مصنوعة من الزجاج النقي لا يتعدى سمكها سمك الشعرة يجمع العديد من هذه الألياف في حزم داخل الكيبلات البصرية وتستخدم في نقل الإشارات الضوئية لمسافات بعيدة جداً .
ويتكون الليف الضوئي من :



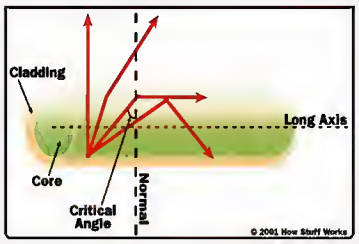
القلب (Core) : وهو عبارة عن زجاج رفيع ينتقل فيه الضوء.

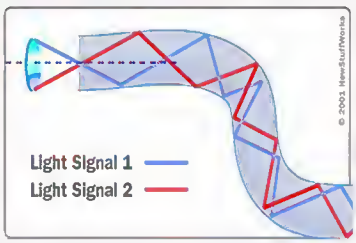
العاكس (Cladding): مادة تحيط بالقلب الزجاجي و هي مصنوعة من زجاج معامل انكساره يختلف عن معامل انكسار الزجاج وتعمل على عكس الضوء مرة أخرى إلى مركز الليف البصري.
مئات أو ربما الآلاف من هذه الألياف الضوئية تصطف معًا في حزمة لتكون الحبل الضوئي الذي يحمى بغطاء خارجي يسمى جاكيت.

الغطاء الواقي (Buffer Coating): غلاف بلاستيكي يحمي الليف البصري من الرطوبة أو ويحميه من الضرر و الكسر.

كيف تتم عملية أنتقال المعلومات في الليف الضوئي

عملية انتقال المعلومات عبر الليف الضوئى هى فكرة بسيطة حيث يتم تحويل الاشارة من صورتها الاولية سواء كانت صوت او فيديو او بيانات الى اشارات كهربية ، ترسل الاشارات الكهربية الى جهاز الارسال او (Transmitter) الذى يحولها بدوره الى نبضات او اشارات ضوئية ، والجزء المسئول عن هذه العملية هو المصدر الضوئى او (Light source) وهو اهم اجزاء جهازالارسال وهناك نوعان اساسيان من المصدر الضوئى هما الليزر دايود (LD) والدايود الضوئى(LED)واي من النوعين يكون مسئولاعن عملية تحويل الاشارة من كهربية الى ضوئية.



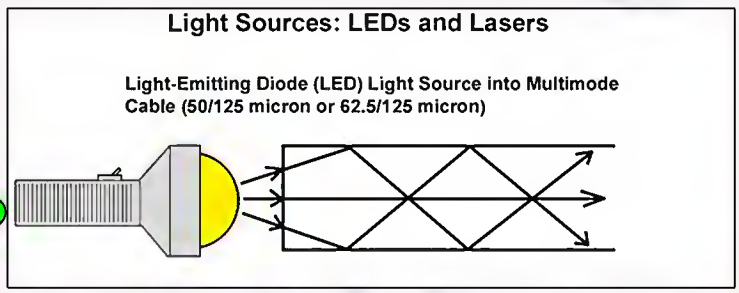


أنواعة

يوجد نوعان من الألياف الضوئية :-

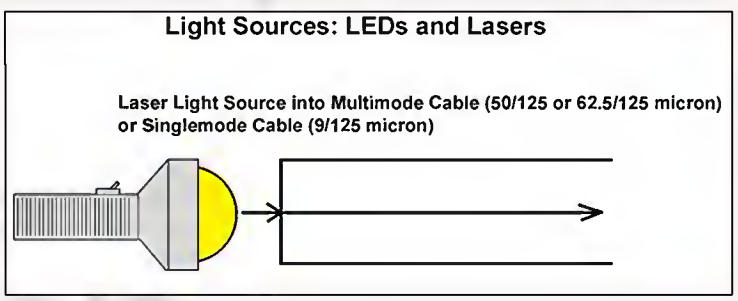
- الألياف الضوئية متعددة النماذج (Multimode)

تنتقل من خلالها العديد من الإشارات الضوئية من خلال الليفة الضوئية الواحدة مما يجعل استخدامها أفضل لشبكات الكمبيوتر.
هذا النوع من الألياف يكون نصف قطره اكبر حيث يصل إلى 62.5micron و تنتقل من خلاله الأشعة تحت الحمراء.

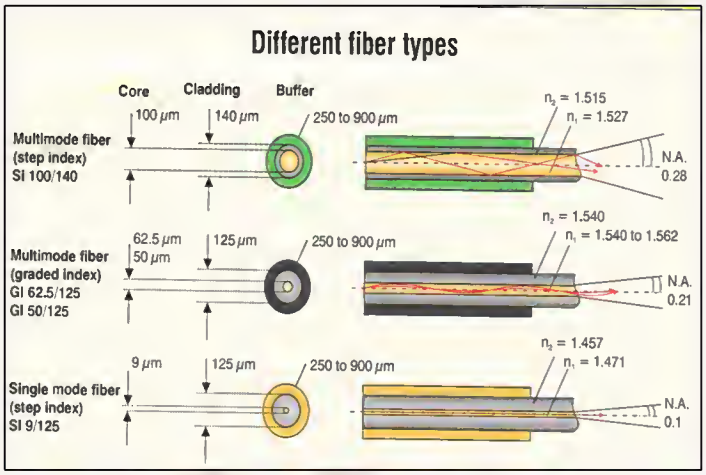


- الألياف الضوئية أحادية النموذج القياسي (Standard Single Mode)

تنتقل من خلالها إشارة ضوئية واحدة فقط في كل ليفة ضوئية من ألياف الحزمة و هي تستخدم في شبكات التلفون و كوابل التلفزيون. هذا النوع من الألياف يتميز بصغر نصف قطر القلب الزجاجي حيث يصل إلى حوالي 9 micron و تمر من خلاله أشعة الليزر تحت الحمراء ذات الطول الموجي 1.3-1.55 nm.



ملاحظة :النوع الأول الخاص بي الألياف الضوئية متعددة النماذج (multimode) يملك نموذجان مختلفان لكن الفكرة نفسها والشكل القادم سوف يوضح أمكانيات ومعايير كل نوع على حدى



انواع واشكال الكونيكتور

- الكونيكتور هو الوسيط بين كابل الفايبر والسويتش ويوجد منة العديد من الانواع والاشكال ولكن الاكثر شيوعا فى عالمنا (ST-FC-SC)

سنة أولى شبكات

بقلم: محمود عز الدين عبدون

سؤال دائما يطرحه الكثير من الشباب أريد أن ادرس الشبكات كيف أبدا وماذا أفعل ثم تمر فترة الدراسة الأولى وبعد ذلك يطرح الشباب سؤال تانى ياجماعة انا اخدت كورسات فى الشبكات كذا وكذا وأريد أن أعمل بس الشركات بتطلب خبرة ماذا أفعل لحل هذه المشكلة؟.ومن وحي هذه الاسئلة أقدم لكم هذا المقال في محاولة مني لتبين أهمية المرحلة الأولى ,فكثير من الشباب ممكن يكون اخدت كورسات بس نظري والنظري لوحده ليس كافي لازم يشتغل بإيده ويمارس كل ما تعلمه لذلك لازم يعرف ماذا يفعل.

لناخد الموضوع من بدايته السؤال الأول :

ماذا يتوجب علي دراسته ؟ , ونصيحتى لك هى دراسة كورس network + ثم A+ وسوف يستغرقوا معك 3شهور , وبهذه الطريقة تكون قد وضعت حجر الأساس وبعدها سوف تجدأمامك مساران مايكروسوفت وسيسكو وانا بفضل شخصيا البدء بمايكروسوفت لانها اسهل وغير ذلك لايوجد شركة فى العالم تخلوا من منتجات مايكروسوفت وحتى لاأطيل عليك فى المقدمة انصحك بقراءة مقالة المهندس عادل الحميدي " من اين ابدأ وكيف ابدأ فى الشبكات سؤال لطالما حيرنى " ففيها الاجابة الشافيه لهذا السؤال ؟.

خلاصة الكلام الآن أنتهيت من دراسة Network +و A+ و MCSA وهى الأولى او Network + و A+ و CCNA وهذا مبدئيا حتى تتمكن من العمل فى مجال الشبكات وتستوعب العمل بعد ذلك إن شاء الله تعالى.

وهنا يأتي السؤال الثانى :

انا اخدت كورسات شبكات وأريد أن أعمل في مجال الشبكات !ماذا أفعل ؟؟؟

1- وهنا سوف تجد أمامك شركات كمبيوتر كبيرة وشركات عادية بها قسم IT ويفضل انك تعمل فى البداية فى شركات عادية بها قسم IT بالشركة, لان شركات الكمبيوتر غالبا ما تقدم الخدمات للعديد من الشركات لذلك الخبرة وأتقان العمل سوف تكون أحد أهم الشروط فيها.

2- فى البحث عن عمل ركز على الشركات العادية كما ذكرنا مسبقا وحاول ترسل ايميلات كثيرا وطبعا سوف تكون بعد اعداد السيرة الذاتية الجيدة (سوف يكون لها موضوع مخصص) أو تذهب بنفسك للشركات تعمل طلب توظيف مع الاستعداد بالمظهر الجيد , فالمظهر هو أول إنطباع يؤخذ فى الاعتبار فهى علامة على شخصيتك .

3- عندما تبدأ بعمل المقابلات لاتيأس لو لم تجد عمل بسرعة لان هذا الشيء ليس جديدا وتذكر قول رسول الله صلى الله عليه وسلم (تفائلوا بالخير تجدوه) صدق رسول الله صلى الله عليه وسلم .

4- اثناء اجرائك للمقابلات هتتعرف من الشركات وهتعرف من الاسئلة ماهي اهم البرامج المطلوبة فى السوق يعنى سوف يصبح عندك فكرة جيدة لمتطلبات السوق الفعلية وصدقني هذه النقطة مهمة جدا .

5- ضع فى إعتبارك لاتضع للراتب الأهمية الكبيرة عند البحث عن عمل , انت تبحث عن خبرة تدعم معرفتك النظرية أولا يعنى بالعربى تضع نصب عينيك كيف تأسس نفسك فقط , وفي نفس الوقت لاتقلل من نفسك او من الراتب ولكن قصدى لاترفض الراتب القليل لوكانت الخبرة كبيرة جيدة وتقدر تبنيك كمهندس شبكات , وهيقدر كلامى اللى بيحب مجال الشبكات بجد وعاوز ياخد خبرة.

طيب تمام اشتغلت فى المجال ودخلت الشركة وجلست بين السيرفرات والاجهزة ..... تمام.. الحمد لله .

هذه بعض النقاط التى من الضروري تاخد بالك منها فى عملك فى مجال الشبكات خصوصا فى اول سنة لان مثل ماقلت لك تأسس نفسك صح إن شاء الله تعالى :-

1- البحث :معظم العمل سوف يعتمد على مهارة البحث وكيفية استخراج المعلومة والبحث عن حل , يوجد كتاب انصحك به اسمه "اسرار وخفايا جوجل" للمهندس مأمون نعيم والذي سوف يتكفل بتعليمك كيف تستخدم محرك البحث جوجل اقوى محرك بحث فى العالم عدد صفحات الكتاب 350صفحة, كتاب فعلا ممتاز .

2- ايجاد الحلول للمشاكل: وهذه تعتبر اساس الشبكات لان المشاكل كثيرا ولازم تعرف كيف تجد حل لكل مشكلة ورويدا رويدا ان شاء الله تكتسب مهارة حل المشاكل بس اهم شيء الهدوء .

3- سد الثغرات : اثناء عملك سوف تجد نفسك فى أشياء كثيرة لاتعلمها وأشياء نسيتها لذا لازم هنا تقرأ دائما حتى تسد كل جانب نقص تجده عندك ويوجد منتديات مثل عرب هاردوير ومركز بوابة العرب من الممكن أن تستفيد منها في هذه النقطة .

4- ملاحظة الاعلى خبرة : دائما أعطي الأنتباه الأكبر للأقدم منك فى العمل وحاول تدرب نفسك على كل شيء يقوم به ولاتنسى أن تتابع كيفية حله للمشاكل التى تواجه

5- اللغة : من المؤكد أننا لن نتجاهل أهمية اللغة الانجليزية فالتكنولوجيا تأتى من الغرب, لذا لو كانتك لغتك ضعيفة فحاول أن تدرب نفسك أكثر وحاول تتابع المواقع التقنية التخصصية للوقوف على آخر التقنيات والتطورات .

http://www.ehow.com/information_1016_computer-networking.html

http://www.computerhope.com/

http://www.about.com/compute/

وتستطيع أيضا إيجاد حلول لمشاكلك من المواقع المذكورة وبهذه الطريقة تضرب عصفورين بحجر تجد حل مشكلتك وتدرب نفسك على اللغة .

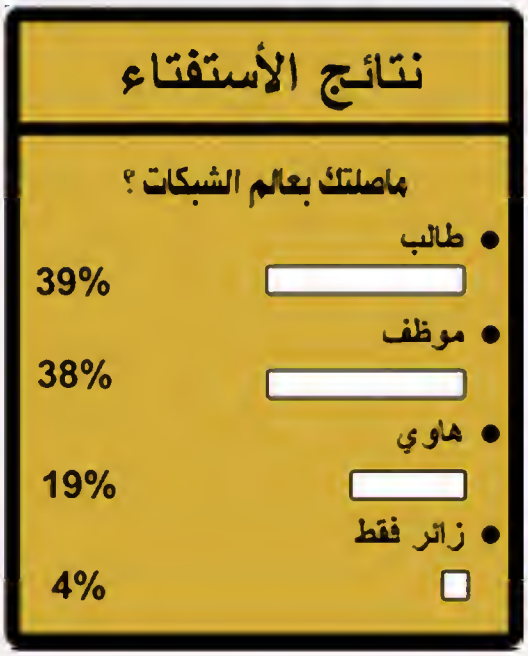
وآخيرا أدخل على الموقع التالي وهو خاص بتعلم اللغة الأنكليزية ويحوي على دروس في مجالات مختلفة بالأضافة إلى أمكانية سماع النطق الصحيح للكلمات, ويوجد صفحة بالموقع ترشدك لطريقة الاستذكار ويوجد منتدى للتفاعل وطرح الأسئلة , وللعلم هذا الموقع ب 16لغة غير العربية .

http://www.ar.talkenglish.com/

وأخيرا اقرأ كثيرا تتعلم أكثر

نتائج الأستفتاء الشهري

الأستفتاء الذي قمت به هذا الشهر كان بهدف معرفة نوعية الزوار التى تزور المدونة وماهي الصلة التى تربطها بعالم الشبكات فمع 350صوت تقريبا أغلقت الأستفتاء وكلي فرحا بالنتائج لان أولا أعداد المصوتين بدأت بالأزدياد مع العلم أن أعداد الزوار اليومي فقط أضعاف أضعاف هذا الرقم لكن الحمد لله على كل شيء وثانيا التوقع المبدأي الذي وضعته فقد توقعت أن تكون نتائج الأستفتاء هي فوز الطلاب بشكل كبير لكن النتائج كانت بعكس توقعاتي أيضا هذا الشهر وقد حمدت الله أن هناك نسبة كبيرة من العاملين في قطاع الشبكات يزور المدونة لان هذه نقطة أيجابية في صفهم لان الأمر يدل على أن هؤلاء الأشخاص يحاولوا تطوير قدراتهم ويزيدوا من معلوماتهم بشكل أكبر في هذا المجال الذي أرى أن لاحدود له وخصوصا أن هناك أناس يعملون ويدعون أن العمل يأخذ كل وقتهم ولايستطيعوا أيجاد متسع من الوقت للقراءة لذا أنا أحيي كل طالب علم يحاول أن يطور نفسه أما للطالب فأنه سوف أقول له شيئا واحد فقط "سحقا لكل طالب علم أكتفى بعلمه " ومعناه أن تحرص على الدراسة والتعلم كل يوم ومهما كانت المراحل التى سوف تأتي عليك لان العلم والتعلم هي حرب القرن الحادي والعشرين فكن دائما مستعد للحرب .



CALL PICKUP

بقلم: أحمد الشحات

سوف نستكمل في هذه المقالة حديثنا عن بعض الخواص الموجودة على أجهزة سيسكو والتى بدأناها بالحديث عن خاصية **Call Park** في العدد القادم واليوم سوف نتحدث عن خاصية لاتقل أهمية عن هذه الخاصية وهي

Call Pickup

طبعا اخواني الاعزاء من اسم العنوان عرفنا ان الهدف منها هو التقاط المكالمة وهذه الخاصية تكون مفيدة فى حالة وجود أكثر من موظف فى نفس المكتب لنضرب مثال بسيط أنت تعمل فى المبيعات وانت غير موجود على مكتب وقام احد العملاء بالاتصال بك

هل ستضيع طلبية الشراء على الشركة بسبب عدم وجودك

بالطبع لا

فبمجرد سماع جرس التليفون سيقوم احد زملائك الموجودين فى نفس المكتب بتغطية زوغانك وهروبك من العمل وبمجرد الضغط على زر Pick up ستنتقل له المكالمة على تليفونه الخاص ولن يضطر للقيام والرد عليها من على مكتبك

سؤال : هل هناك أنواع من Call Pickup أم انها نوع واحد رن الجرس وسحب الخط

الاجابة : هناك ثلاث أنواع

Call Pickup -1

وفي هذا النوع يستطيع المستخدم أن يلتقط المكالمة الواردة على أى تليفون ولكن يشترط أن يكون فى نفس المجموعة

كل ما على المستخدم فعله هو أن يقوم بضغط Pickup Softkey ويقوم CUCM اتوماتيكيا بطلب رقم Pickupالمناسب المرتبط ب DN المطلوب وبما أن التليفون الأخر موجود فى نفس مجموعة Pickupفأن المكالمة الواردة سيعاد توجيهها الى التليفون الذي تم ضغط Pickup Softkey عليه

Group Call Pickup-2

فى هذا النوع يستطيع المستخدم ان يلتقط المكالمات الواردة الى DN's موجودة فى مجموعة Pickupأخرى

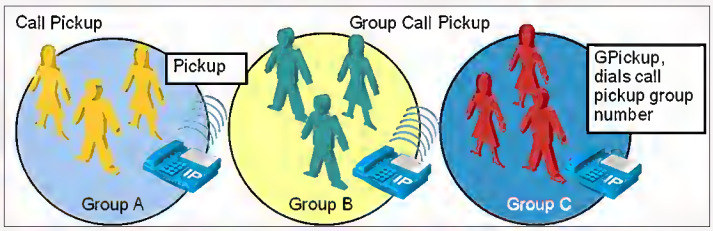
كل ما على المستخدم فعله فى هذا النوع هو ضغط GPickup Softkey ثم الاتصال برقم الموعة المناسب الذي يرن فيه التليفون المراد سحب الخط منه

Other group Call Pickup-3

في هذا النوع يستطيع المستخدم التقاط المكالمة من مجموعة أخرى مرتبطة بمجموعته وفي بعض الأحيان يشار الى ذا النوع على أنه Pickup chaining

وكل ما على المستخدم فعله هو ضغط OPickup Softkey

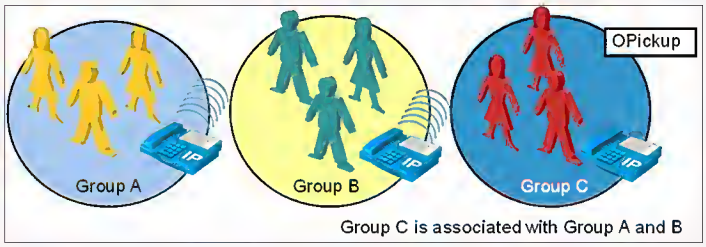
أمثلة على هذه الأنواع



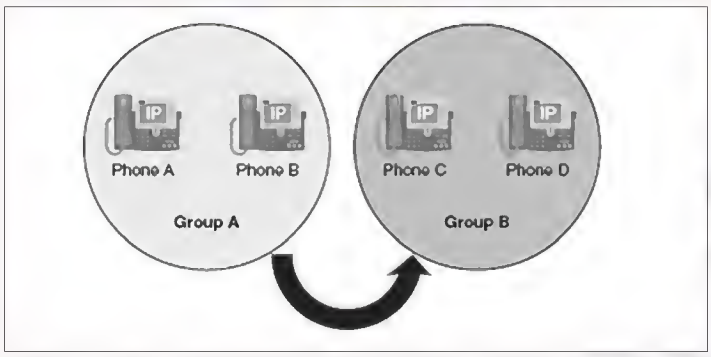
كما نرى من ألوان المجموعات فكل لون هو مجموعة منفصلة نستخدم فقط Pickup softkey أما بين الألوان المختلفة فنستخدم الزر Gpickup

Other Group Call Pickup

في هذا الشكل نرى ان المجموعة C مرتبطة بالمجموعتين A و B لذا سنستخدم الزر Opickup



مثال على كيفية عمل الثلاث أنواع



المجموعة A رقمها 1111وينتمي لها التليفونين A & B والمجموعة B رقمها 2222وينتمي له االتليفونين C&D

فى حالة لو أتت مكالمة الى التليفون A فيستطيع التليفون B سحب المكالمة بمجرد ضغط الزر PICKUP فقط

أما لو أتت مكالمة على أحد التليفونين C أو D فيجب على المستخدم فى المجموعة A أن يضغط زر GPICKUP أولا ثم يتصل بالرقم 2222 حيث أن هذا هو رقم المجموعة ثم يضغط Answer بعد ذلك لكي يجيب على المكالمة

وبالمثل لو كانت المكالمة فى المجموعة A ويرد أحد المستدمين فى المجموعة B سحب الخط فيضغط أولا على الزر Gpick ثم يتصل بالرقم 1111حيث أن هذا هو رقم المجموعة الأولى

سؤال : ماذا سيحدث أذا كان هناك أكثر من تليفون يرن فى نفس المجموعة ماهي المكالمة التي ستلتقط وما هي المكالمة التي ستترك ؟

الاجابة : المكالمة التي ستلتقط هي المكالمة التي ترن منذ مدة اطول من الأخرى بمعنى أخر المكالمة التي أتت اولا تلتقط أولا

سؤال :لو عندنا أكثر من مجموعة مرتبطة ببعض مثل A&B&C داخل X لمن ستكون الأولوية لالتقاط المكالمات

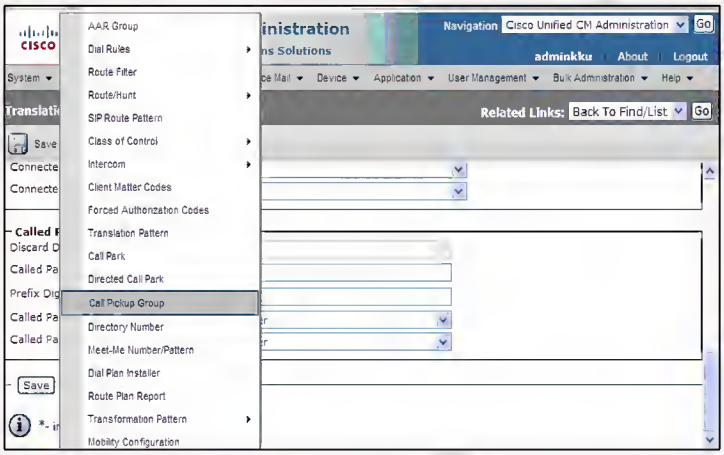
الاجابة: ستكون الأولوية لترتيب المجموعات داخل المجموعة الأم X أي ستكن A هي الأولى وبعدها B وهكذا

Call Pickup Configuration

لعمل اعدادات call pickup يجب أولا عمل رقم ل call-pickup ثم نربطه ب DN

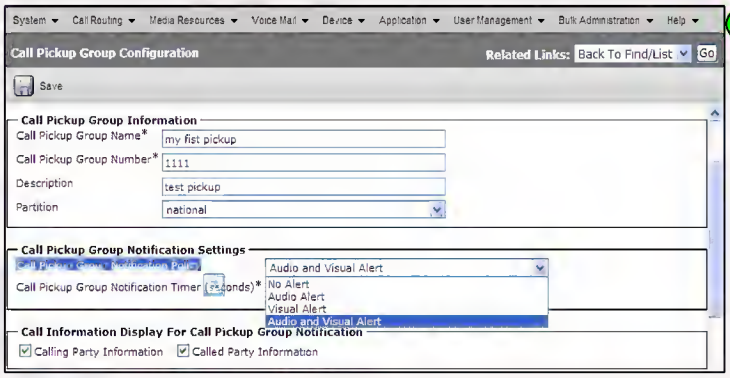
Call Routing -----> Call Pickup Group --->Add New

وتابع بعدها معي بالصور

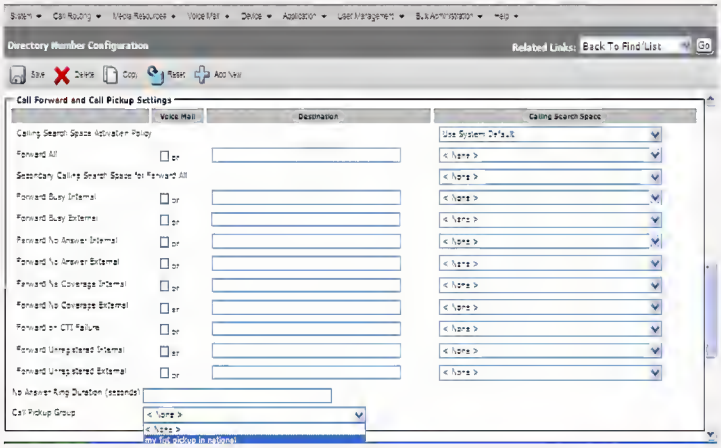


نضع اسم فريد لا يتكرر ورقم فريد أيضا لا يتكرر فى خانات الاسم والرقم

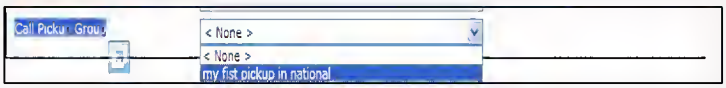
ملحوظة : فى خانة Partition لو تم وضع أى قيمة فأن هذا يمنع التليفونات الى في CCS التي لا تحتوي على هذا ال Partition من التقاط المكالمة وبالنسبة لخانة Call Pickup Group Notification Policy بها اختيارات عدة سواء تنبيه صوتي او مرئي او عدم التنبيه أصلا نختار منها ما يناسبنا



ولكي نضيف الأرقام التي نريدها لهذه المجموعة نذهب الى DN وتحت العنوان Call Forward and Call Pickup Settings وفى اخر خانة نجد Call Pickup Group نختار اسم المجموعة التي نريدها وفي حالتنا هذه لم نعمل الا مجموعة واحدة لذا لن نجد غيرها !.



وهذه صورة أقرب

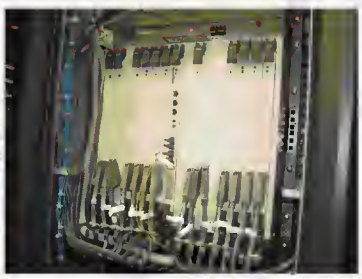


عند الاتصال بأحد التليفونات التي فى المجموعة فبعد 6ثواني سيعطيك التليفون الاخر الذي لا يرن لمبة حمراء من السماعة وصوت موسيقى لينبهك بوجود مكالمة على التليفون

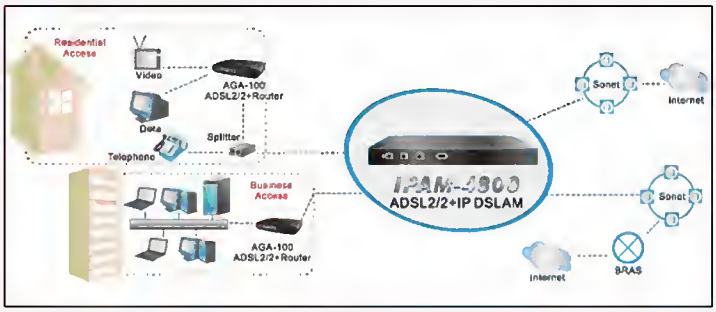
ملحوظة : يمكن تغيير قيمة 6ثواني الى أي قيمة تريدها من خانة call (seconds) pickup group notification timer

تعرف على الديسلامات

بقلم: أسلام محمود



الديسلام او Digital Subscriber Line Access Multiplexer) DSLAM)ومعناه باللغه العربيه الخط الرقمى المتعدد الوصول وهو جهاز خاص بالشبكات يتمركز عادة في شركات مقدمي حدمة الأنترنت أو شركات الهاتف ويعد مسؤولا عن عملية دمج خطوط الهاتف مع خدمة الأنترنت بالأضافة إلى أمكانية انشاء اكثر من اتصال فى وقت واحد مع اكثر من عميل او مع اكثر من مودم دى اس ال .



ويقوم الديسلام بتوفير بعض الخدمات من dsl مثل Adsl, SHDSL,VDSL وسنكتفى بذكرهم فقط في هذا المقال وسوف أعود لكي أشرح كل واحد منهم على حدى في الأعداد القادمة من المجلة أما الأنواع والشركات المصنعة لهذا الجهاز فهي كثيرة نذكر بعضا منها d-link, c-com, Alcatel,Huawei وهناك شركات اخرى ولكن تم ذكر الشركات الاكثر انتشارا فى هذا المنتج.

وتنقسم الديسلامات حسب احجامها هنالك ديسلامات تحتوى على 16بورت و 32بورت و 64بورت وكلما ارتفع حجم البورتات كلما زاد عدد المستخدمين عليه وازدادت كفاءة الديسلام .على اليسار صورة لديسلام صغير 16بورت من D-Link وعلى اليمين صوؤة لديسلام كبير يملك بورتات أكثر

أما السرعات المتاحة تعتمد بالمقام الأول على بعد العميل عن الديسلام وهي تحسب وفقا للجدول القادم

- 25 Mbit/s at 1,000 feet (~300 m)
- 24 Mbit/s at 2,000 feet (~600 m)
- 23 Mbit/s at 3,000 feet (~900 m)
- 22 Mbit/s at 4,000 feet (~1.2 km)
- 21 Mbit/s at 5,000 feet (~1.5 km or ~.95 miles)
- 19 Mbit/s at 6,000 feet (~1.8 km or ~1.14 miles)
- 16 Mbit/s at 7,000 feet (~2.1 km or ~1.33 miles)
- 1.5 Mbit/s at 15,000 feet (4.5 km or ~2.8 miles)
- 800 kbit/s at 17,000 feet (~5.2 km or ~3.2 miles)

مع العلم ان الديسلام يستخدم تقنية) Asynchronous Transfer Mode (ATM فى نقل البيانات .كما يمكن للديسلام توصيله من خلال fastetheret او عن طريق fiber optic . اما عن التقنيات التى يقوم بتوفيرها فهو يدعم ال vlans ويدعم ايضا routing حيث من الممكن استخدامه بدون توصيل روتر فى بيئة ISP ومن الممكن تكوين pppoe server or pppoa server عليه ايضا مما يرفع من امكانياته .ويتعامل الديسلام بشكل رئيسى مع قطعة الاسبليتر التى من خلالها يتم توصيل الانترنت من خلال خطوط الهاتف الارضى حيث ان الاسبليتر يستطيع الفصل بين حرارة التليفون والانترنت مما يجعل له دور مهم فى خدمة adsl .واتمنى ان يكون هذا المقال البسيط قد أجاب على بعض أسالتكم حول كيفية عمل دمج خطوط الأنترنت مع خطوط الهاتف وسوف نتطرق في الاعداد القادمه من المجله أن شاء الله معلومات أكثر عن هذا الجهاز .

IGMP

Internet Group Management Protocol

لكي تقوم الروترات بتمرير الترافيك الخاص بي الـ Multicast إلى الشبكات المتصلة معها تحتاج هذه الروترات أن تعرف من هي الأجهزة أو الـ Client التى ترغب بهذا الترافيك لذا حديثنا اليوم سوف يكون عن البروتوكول المسؤول عن إدارة هذه العملية وهو الـ IGMP والذي يتم من خلال إرسال العميل طلب إلى الروتر بواسطة هذا البروتوكول لكي يصل إليه ترافيك الـ Multicast .

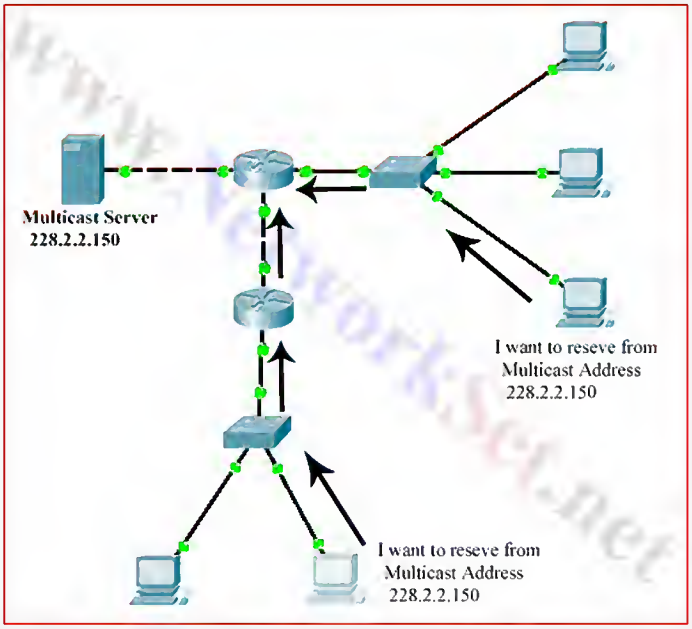
مقدمة

الـ IGMP أو Internet Group Management Protocol أول من طور هذا البروتوكول هو Steve Deering عام 1986في الـ RFC 988 وبعدها خضع هذا البروتوكول لعدة تطويرات وتحديثات على يد نفس الشخص ليقوم أولا بتطويره إلى الـ IGMPv1 في الـ RFC 1112وبعدها إلى الـ IGMPv2 في الـ RFC 2236وآخيرا الصيغة الآخيرة منه الـ IGMPv3 في الـ RFC 3376كما يعد Steve Deering أحد مطوري بروتوكول الـ IPv6 والذي ألتحق عام 1996بشركة سيسكو للعمل فيها وهذه صورة له

وظيفة بروتوكول الـ IGMP

لكي يصل الترافيك الخاص من المصدر إلى الأجهزة يحتاج هذا الأمر إلى وجود مجموعة تضم الأجهزة والسيرفر الذي يولد هذا الترافيك والتى يعبر عنها بأحد أيبيات الملتي كاست والتى نعرفها بأنها تنتمي للكلاس D والتى قامت الأيانا بحجز نطاق من الأبيبي خاص بها يبدأ بي 224.0.0.0ويبنتهي 239.255.255.255

ولكي تضمن هذه الاجهزة وصول الترافيك تحتاج أن ترسل طلب إلى الروتر الذي يمثل الـ Gateway الخاص بها مخبرة أياه بأنها تريد الأنضمام إلى هذه المجموعة وبالتالي يقوم الروتر بتمرير هذا الترافيك إليها ولكن السؤال الذي يطرح نفسه كيف يتم إرسال هذا الطلب ؟ لكي تضمن هذه الأجهزة الأنضمام إلى هذه المجموعة تحتاج أولا إلى برنامج خاص يثبت على أجهزة العملاء وهو عادة أما يكون برنامج عرض فيديو أو برنامج صوتي من أجل الراديو مثلا والتى عادة ماينحصر أستخدام الملتي كاست فيها)فيديو أو راديو عبر الشبكة(وفيها يقوم البرنامج باخبار كرت الشبكة NIC برقم المجموعة الذي ينتمي إليها والذي يعبر دائما برقم الأيبي ملتي كاست وعندما يستلم كرت الشبكة رقم الأيبي يقوم أوتماتيكيا بأرسأل الطلب إلى الروتر مستخدما بروتوكول الـ IGMP وهذه صورة توضح الفكرة



خلاصة هذا الكلام : يستخدم الـ IGMP في تسجيل الـ Client إلى الروتر وهذا يشمل عملية الـ Joining وعملية الـ Leaving الخاصة بي الـ Multicast Group لذا إستخدامه ينحصر فقط بين العميل والروتر.

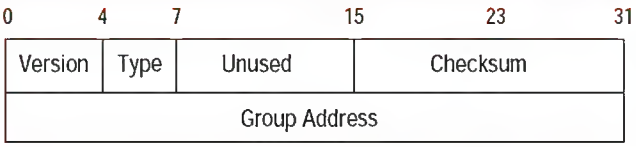
وكما أوضحت في بداية التدونية أن لهذا البروتوكول 3إصدارات مختلفة وهي

IGMPv1

يملك هذا الأصدار نوعان أثنان من الرسائل فقط

الأول : Membership Query وهي ترسل من خلال الروتر فقط وكل 60 ثانية وهي من اجل إعلام الأجهزة أو العملاء بوجود Multicast Traffic داعيا أياهم للانضمام إليها وهي ترسل على العنوان 224.0.0.1ومن خلال كل منفذ أو Segment موجودة

الثاني : Membership Report يتم إرسالها من خلال العميل فقط ومن أجل الأنضمام إلى المجموعة فبعد وصول الرسالة الأولى من الروتر يقوم العميل بأرسال Report على الأيبي الذي قام بأرسال الـ Membership Query مخبرا أياه برقم المجموعة التى يريد الأنضمام إليها وهي عادة تكون موجودة داخل الـ Header الخاص بي الـ IGMP وهذه صورة توضح الـHeader الخاص بي الـ IGMPv1

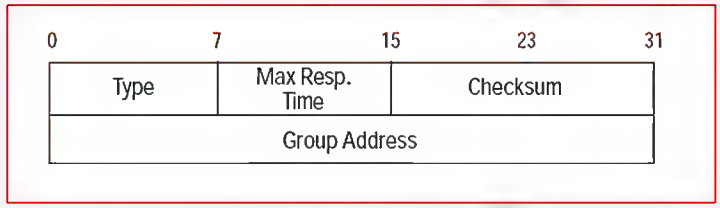


وكما تشاهدون أغلب الخانات مفهومة ماعدا خانة الـ Type والتى تحدد نوعية الرسالة Query or Report وهي أما أن تكون ox11 من أجل الـ Query أو ox12 وهي من أجل الـ Report أما خانة الـ Address Group فهي من أجل إرسال رقم المجموعة التى يرغب العميل بالأنضمام إليها

IGMPv2

في الـ V2 تم إضافة نوع ثالث من الرسائل وهو الـ Leave Group Message وهي ترسل فقط من خلال العملاء على الأيبي 224.0.0.2الخاص بكل الروترات الموجودة على الشبكة وفيها يخبر الروتر بأنه يريد أن يغادر المجموعة وبدوره الروتر يوقف إرسال الترافيك إليه من خلال إعادة إرسال Query Message إلى كل الأجهزة الموجودة حتى يعلم من منهم مازال يريد التواصل مع المجموعة ومن منهم يريد التوقف والتى ترد عليها الأجهزة التى مازالت تستمع لهذا الترافيك من خلال رسالة الـ Report وهي الميزة الأولى بين الأثنان أما الميزة الثانية فهي تتمثل في قدرة الروتر على إرسال صنفان من الـ Query Message فلو فرضنا أن الروتر إستلم طلب مغادرة من أحد العملاء وكما أوضحنا سابقنا بأن الروتر يرد على هذا النوع من الرسائل بأرسال Query Message إلى كل العملاء الموجودين ومن هنا وجدت الميزة الثانية فعوضا عن إرسال Query إلى كل العملاء وبغض النظر عن

المجموعة التى ينتمي إليها هؤلاء العملاء يمكن إرسال Specific Query أي خاص بمجموعة معينة فقط وليس إلى كل الأجهزة الموجودة مع العلم أن الطريقتان متاحتان على البروتوكول أما الميزة الثالثة فسوف تتضح معنا بعد الأطلاع على الـ Header الخاص بي الـ IGMPv2 :



وكما يتضح هنا بعض التغييرات في الـ Header فقد تم أضافة خانة جديدة وهي Max response time وهي من أجل أخبار العميل بالمدة الزمنية التى يجب أن يرد عليها أثناء أرسال الـ Query وهي عادة تكون ثانية واحدة , أما الميزة الرابعة فهي من أجل تحديد الروتر المسؤول عن عملية إرسال الـ Query وفيها يقوم الروتر الذي يملك أيبي أعلى بأرسال الـQuery بينما يتوقف الثاني عن الأرسال.

النقطة الآخيرة التى أحب أن أشير إليها وهي خانة الـ Type في IGMPv2 وهي كالآتي Query=ox16, Report=ox11, Leave=ox17 .

IGMPv3

يعد هذا الأصدار هو تحديث فقط للأصدار الثاني وفيه تم أضافة ميزة جديدة تدعم عمل Filtering لـ Source Multicast وبكلام آخر تتيح للعميل تحديد الـ Source IP Address الذي يريد أن يستلم منها الترافيك الخاص بالملتي كاست.

كيف تقوم بعمل راديو على الشبكة

بقلم: أيمن النعيمي

متطلبات العمل

برنامج الـ Winamp

أضافة لبرنامج الوينامب SHOUTCAST DSP قم بتحميلها من خلال الرابط التالي

http://yp.shoutcast.com/downloads/

سيرفر SHOUTCAST Server قم بتحميله من نفس الرابط السابق

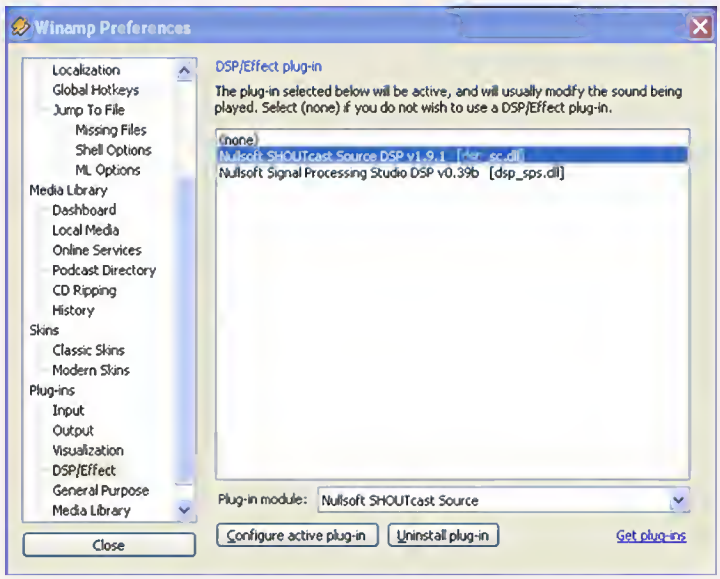
مراحل التثبت

أول شيء قم بتثبيت برنامج الـ Winamp وهو تثبيت عادي لايحتاج إلى احترافية يعني Next–> Next–>Finish بعد الأنتهاء من تثبيت البرنامج لاتقم بتشغيل البرنامج حتى ننتهي من تثبيت الأضافة SHOUTCAST DSP وهي أيضا لا تحتاج إلى شيء فقط Install عادي

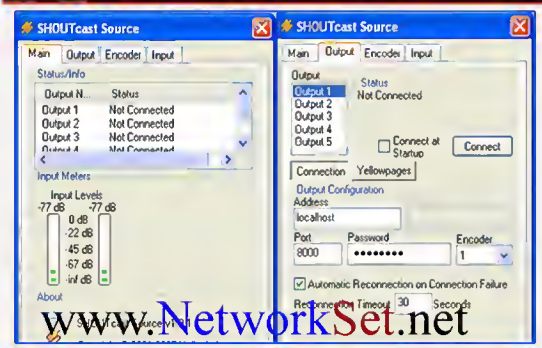
الخطوة الثانية وهي تثبيت السيرفر وهو مهم من أجل عملية المشاركة والـ Broadcasting على الشبكة وهو أيضا لا يحتاج منك إلا الضغط على زر Install

مراحل الأعداد والتشغيل

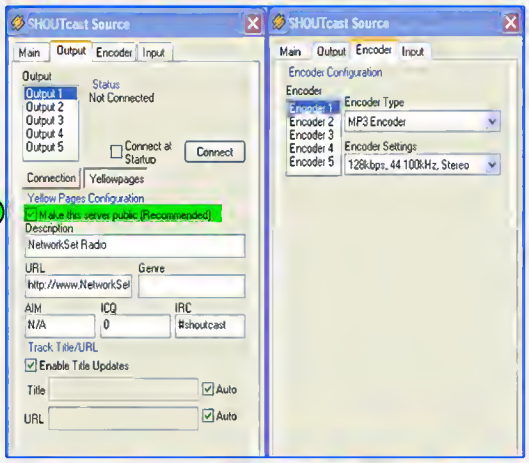
نقوم أولا بتشغيل برنامج الـ Winamp ونقوم بالضغط على زر CTRL+P لتظهر لنا هذه النافذة



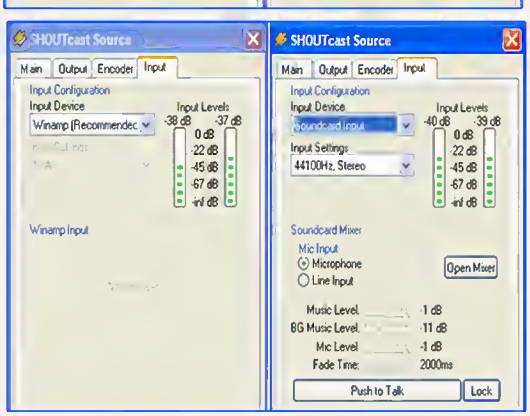
وبعدها نضغط على الأضافة المظللة باللون الأزرق لتظهر بعدها الأضافة الخاصة إلى السيرفر والذي بدوره يقوم Winamp بأرسال الموسيقى من برنامج الـ بأرسال الموسيقى إلى باقي الأجهزة التى تريد الأستماع وهذه بعض الصور توضح كيفية أعداد وتجهيز الأضافة



هنا لانقوم بتغيير أي شيء إلا لو في حال أردت تغيير المنفذ الذي سوف يتم من خلاله أستلام الـ Stream الخاص بالراديو وهو كما موضح يعمل على المنفذ 8000

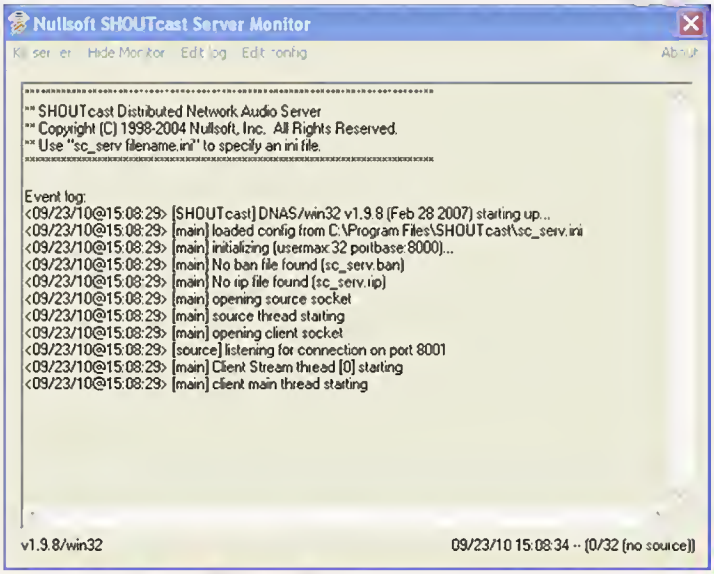


نقوم أولا بوضع أشارة على الصندوق المظلل بالأخضر وتستطيع وضع Description للراديو لو في حال كان لديك أكثر من واحدة أما في الصورة الثانية فهي من أجل تحديد نوعية ودقة الصوت ويفضل أن تكون MP3 وبدقة 128 Kbps



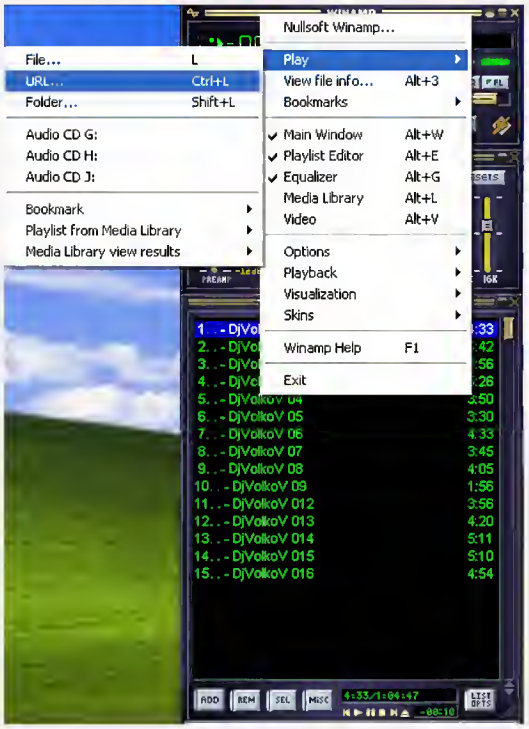
وآخيرا نستطيع أن نحدد من أين يجب أن يكون مدخل الـ Stream لو في حال أردت أن يكون من برنامج آخر غير الـ Winamp أو لو في حال أردت أن تقوم بربط الـ Stream مع المايكروفون مباشرة

بعد الأنتهاء من الأعدادت نقوم بتشغيل السيرفر تستطيع أن تجده من خلال التوجه إلى Start-> All Program ->SHOUTcast DNAS (GUI) ->SHOUTcast DNAS



بقي علينا خطوة واحدة وهي التوجه إلى الأضافة والضغط على زر connect ليبدأ الـ Streaming وبهذه الخطوة نكون قد أعددنا السيرفر وهو الآن بدأ الـ Streaming أو البث

وآخيرا نطلب من الأشخاص الموجودين على الشبكة من تشغيل برنامج الـ Winamp أو Windows Media Player وعمل كما هو موضح بالصورة



وبعدها سوف يظهر لك صندوق صغير نكتب فيه عنوان السيرفر أو الجهاز الذي يقوم بعمل البث متبوعا برقم المنفذ وهذا مثال 192.168.1.1:8000 بالنسبة لي WMP نتجه إلى File-- >Open URL ونكتب فيه عنوان السيرفر وعلى الشكل التالي Http:// 192.168. 1.1:8000

ومبروك عليك محطة الراديو

نظام المراقبه بالشبكات
Network Surveillance System

بقلم: أحمد الجلجولي

عند التفكير بتركيب نظام مراقبه بالكاميرات لحمايه منشأه معينه فمن الاولويات النظر إلى الموقع المراد مراقبته لأنه وفي بعض الاحيان لا يمكن تركيب نظام مراقبه تقليدي (ذو الاسلاك الاحاديه Coaxial Cables) ويعود السبب في ذلك الى طبيعه الموقع ولحل مثل هذا العائق تطلب وجود نظام اخر يحل مكان النظام التقليدي ويكون بنفس الكفائه , ومن خلال التطور التكنولوجي وجدت حلول منها الجيد ومنها السيء والمقياس الذي نحكم به على النظام اهو جيد ام سيء هو التوافق بينه وبين الموقع لدينا فمن الممكن ان يكون نظام سيء في موقع ولكن يكون في اعلى كفائته في موقع اخر , ومن هذه النقطه جاء نظام جديد يلبي كافه الاحتياجات ويكون مناسبا لاغلب المواقع وهو موضوعنا والذي سوف نتحدث عنه ويسمى بنظام المراقبه بالشبكات , و سمي بهذا الاسم لانه يستخدم شبكه الحاسوب كوسيله لنقل البيانات , وتتضمن هذه البيانات عاده إشاره الفيديو وبعض احتياجات النظام الاخرى , ويتكون هذا النظام من كاميرات مراقبه تحتوي كل منها على كرت شبكه ليتم ربطها من خلاله , وتتم المراقبه إما عن طريق متصفح الانترنت او عن طريق برنامج خاص يتم تنصيبه على إحدى اجهزه الحاسوب للمراقبه من خلاله .

ومن مميزات هذا النظام انه يقوم بتقديم كفائه النظام التقليدي , ولا تحتاج الى كوابل جديده او اعمال تركيب كثيره فبكل بساطه يربط بأقرب نقطه شبكه بجانبه ولا يحتاج الى جهاز حاسوب خاص به بل بالامكان المراقبه عن طريق اي جهاز على الشبكه وشخصيا اعتبر هذه النقطه من اكبر مساوئ هذا النظام , فالافضل لأي نظام مراقبه بالكاميرات توفر جهاز حاسوب خاص به , ومن المميزات الاخرى التي نذكرها هي سهوله إضافه كاميرات جديدة الى النظام دون الحاجه الى تطوير او عمل اي تعديل على اي جزء من اجزاء النظام الاخرى .

ومن افضل خصائص هذا النظام هي خاصيه الـPOE وهي اختصار لـPower Over Ethernet وتعني خاصيه التزود بالطاقه عبر الشبكه اي ان النظام لا يحتاج الى محولات كهربائيه او اي مزود طاقه اخر فبفعل هذه الخاصيه يتم تغذيته عبر الشبكه .

ومن نقطه ان هذا النظام هو نظام حمايه فتتوفر به خطوط دفاع عنه وتتلخص بالامن ومنع اي شخص غير مخول بالدخول عليه من خلال نظام حمايه خاص به يتم برمجته بحسب الرغبات والمتطلبات الشخصيه , ومن إحدى هذه الخصائص خاصيه منع رقم الاي بي اي ان النظام يمكن برمجته ليسمح فقط للاجهزه المختاره بالدخول عليه .

وفي حاله اردت استخدام جهاز خاص للنظام فيلزمك برنامج مراقبه يقوم بعرض كافه الكاميرات المتوفره على الشبكه وفي هذه الحاله يطلق على هذا الجهاز إسم جهاز التسجيل عبر الشبكه NVR: Network Video Recorder ومن المميزات التي يقدمها هذا البرنامج التسجيل بالحركه و نظام إنذار و سهوله الاستخدام ومراقبته من مواقع اخرى بكل سلاسه .

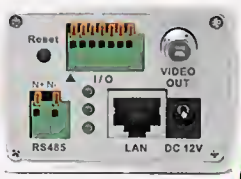
ولتكتمل فكره نظام الحمايه والمراقبه يجب النظر الى ما يسمى بالتسجيل وتعتبر هذه النقطه من اهم مراجع الحمايه ونعني بالتسجيل اي هي تلك الاليه التي يمكن من خلالها القيام بحفظ كافه الاحداث على النظام وإما ان تكون هذه الاحداث على شكل صور متحركه) الفيديو (او ان تكون تسجيلا للصوت او ان تكون احداث كتابيه ولكل حدث من هذه الاحداث اليه للتسجيل تختص به فمثلا اليه تسجيل الاحداث الكتابيه تختص بعمل مذكره يتم من خلالها تسجيل كافه احداث النظام نصيا وتسمى هذه الاليه بـ Event Log Recorder وتعني مذكره الاحداث النصيه ويمكن تطبيق كافه عمليات القراءه عليها من نسخ و استعراض علما بأنه يمكن حذفها ولكن في حاله الحذف يتم كتابه حدث مميز يبين بأنه تم إجراء عمليه حذف .

والان لنلقي نظره الى الاليه التسجيل الصوتي Sound Recording Utility ولا تتوفر هذه الاليه في كافه انظمه الحمايه وهي بالطبع متوفره بنظام المراقبه بالشبكات ومن اعمالها تسجيل الصوت من خلال الميكروفونات والتي تكون مدعومه بداخل الكاميرات , وايضا يمكننا من خلال هذه الاليه عمل محادثات صوتيه بين مراقب النظام والشخص المراقب .

ولننتقل لاليه تسجيل الفيديو وهي المرجع الرئيسي للاحداث فيمكن الاستغناء عن كافه الاليات الاخرى وندع الصوره تتكلم ويتم تسجيل هذه الاحداث من خلال عده وسائل منها التسجيل بالحركه Motion Recording او التسجيل الدائم All time Record-ing او التسجيل اليدوي Manual Recording .

وتشترك جميع الاليات السابقه بموقع حفظ المعلومات وهو القرص الصلب وتعتمد مده حفظ هذه المعلومات على القرص الصلب بسعته فالعلاقه طرديه فكلما زادت السعه زادت مده الحفظ ويمكن التحكم بزياده مده الحفظ ايضا من خلال اليات التسجيل فيمكن مثلا برمجه اليه التسجيل بالفيديو لتقوم بالتسجيل من خلال الحركه ويمكن ايضا عمل تقليل لجوده الصوره وتؤثر مباشره على زياده مده الحفظ .

وبهذا تكون قد تكونت لديك عزيزي القارىء فكره ونقاط رئيسيه يمكنك من خلالها الاجابه عن سؤال يدور في خاطرك الا وهو هل يصلح نظام المراقبه بالشبكات للموقع لديك ام لا فإذا كانت الاجابه نعم فبكل سهوله بإمكانك القيام بتركيب هذا النظام بكل سهوله اما إذا كانت الاجابه لا فأنت تحتاج الى نظام اخر ليلبي احتياجاتك وفي حاله الحيره يمكنك سؤال شخص مختص بهذه الامور واخباره عن سيناريو الموقع لديك وتدعه يختار ما هو مناسب لديك .



Linux Redundancy

بقلم: أحمد بخيت

السلام عليكم ورحمة الله وبركاته – كيف حالكم جميعاً أتمنى أن تكونوا جميعاً بخير وتتمتعون بتمام الصحة والعافية – إني اكتب إليكم اليوم من مصر الغالية – ارض الكنانة ارض خير أجناد الأرض – صدق رسول الله صلى الله عليه وسلم – ويوجد احتمال كبير أن يكون العدد القادم اكتب إليكم من بلاد النوعية والتعددية وبلد التقنية – أرجو منكم الدعاء بالتوفيق والتثبيت.

كما انه أود أن اشكر صديقي الغالي ايمن لإتاحته الفرصة للصغار أمثالي بان يكتبوا جنباً إلى جنب إلى العمالقة في هذه المجلة – اسأل الله عز وجل أن يجعل ثواب نشر هذا العلم في ميزان حسناته وحسنات الإخوة العمالقة في هذا الصرح.

كما انه أود أن أهنئ نفسي وإياكم بأعياد السادس من أكتوبر حيث الانتصارات التي طال انتظارها عسانا نحرر المسجد الأقصى قريباً – مع العلم أن خطوبتي وكتب الكتاب كانوا في هذا اليوم السادس من أكتوبر 2010هذا العام – أرجوكم أن تدعوا لي بالتوفيق.

إما الآن في هذا العدد فاني سوف أتطرق إلى موضوع هام جداً بالنسبة إلى الشركات الكبيرة والمتوسطة وهو التعددية في أنظمة لينكس **Linux Redundancy** إذ انه من الصعب جداً تغطيته في عدد واحد لكن كل ما يهمنا هو طرق باب هذا الموضوع مثله مثل أي موضوع فتحته في كتاباتي التي رزقني الله بها – أهم شئ هو أن تعرف كل شئ عن شئ وان تعرف شئ عن كل شئ.

- لماذا استخدام التعددية ؟؟؟

هذا الموضوع يتم الاستعانة به في العديد من المجالات للشركات الكبرى لعدة أهداف منها إضافة شئ من الاستقرار للخدمات المقدمة إذ انه يتم وضع أكثر من سيرفر لأداء نفس الوظيفة بان يكون احدهم أساسي **Primary** بينما الآخرين يكونوا **Secondary** وعندما يقع أو يحدث فشل في أداء السير فر الأساسي فان السير فر التالي له هو الذي يتولى العمل ويضمن استمرار هذه الخدمات بلا أن يشعر العميل بهذا، كذلك يوجد أسلوب آخر يمكن أن نستفيد منه في هذه التقنية وهي توزيع الأحمال على هذه السيرفرات مجتمعة مثل أن يكون نسبة من الحمل أو الخدمات على السيرفر رقم واحد بينما السيرفرات الأخرى تتشارك نفس النسبة المتبقية أو أن تتشارك كل السيرفرات في المؤسسة لو فرض انه لدينا 5سيرفرات تتشارك كل منها ما نسبته 20% من الأحمال وهذا يؤدي إلى تقديم خدمة مستقرة ويتم تنفيذها بسرعة وإتقان، إما الأسلوب الأخير في هذه التقنية هو توزيع الخدمات حسب أنواعها مثل أن يكون هناك سيرفر مخصص لخدمات الفويس مثل **Asterisk** وآخر خاص بالهوست **Apache** وآخر خاص بقواعد البيانات **MySQL** وهكذا مع أن هذا النوع يفضل استخدامه في الأنشطة المتوسطة وليست الكبرى.

- أنواع التعددية:

عند الدخول إلى عالم التعددية يفضل أن نطلق على هذا العالم اسم Clustering حيث أنها تعني مجموعة من السيرفرات أو الأجهزة التي تتعاون أو تتشارك فيما بينها وفي النهاية تظهر وكأنها جهاز واحد لأداء مهمة واحدة أو هدف واحد – هذا الهدف يمكن أن يكون متعدد أو هدف واحد حسب طبيعة العمل – هذا الجزء يختلف عن الجزء السابق في انه سيكون علمي بطريقة أكثر حدة من الجزء السابق إذ انه يمكن اعتبار الجزء السابق كمقدمة أو شئ عملي لما يتم التطرق إليه في بيئة العمل.

وهنا نجد انه لدينا أربعة أنواع كل منها حسب التطبيق الذي تريد المؤسسة الوصول إليه:

High-availability (HA) clusters

في هذا النوع الهدف الأساسي هو تحسين توافر الخدمات حيث انه يتم عمل مجموعة من العقد – على الأقل عقدتين – التي تستخدم لتقديم الخدمات لتلافي مشاكل نقطة الخطأ الوحيدة Single Point of Failure

Load-balancing clusters

وهي ربط أقسام متعددة لتقاسم أعباء العمل الحاسوبية وهي تظهر وكأنها حاسب واحد منطقياً لكن في الواقع كل جهاز أو سيرفر في هذه المجموعة توكل إليه مجموعة من المهام حيث أن مثل هذا النوع يتم استخدامه لتحسين كفاءة النظام ككل مع الأخذ في الاعتبار أن هذا النوع من التطبيقات يتم استخدامه بكثرة مع مزودي الخدمات مثل الهوستنج أو الانترنت.

Compute clusters

غالباً ما يتم استخدام مثل هذا النوع في الإغراض الحسابية ولا يتم استخدامه في الإغراض العادية حيث انه يستخدم في التحليل بصفة رئيسية مثل تحليل حوادث تحطم الطائرات أو المركبات الجوية حيث الأحكام أو الدقة هي الشئ الوحيد المرغوب من هذه الأنظمة ويتم توكيل كل عقدة أو جهاز مجموعة معينة من الأحداث يقوم بتحليلها بصورة دقيقة جداً ثم في النهاية يتم استخراج تقرير واحد من كل هذه الأجهزة هذا التقرير يساعد في الوصول إلى الحقائق بعد تحليلها

Grid computing

في هذا النوع نلاحظ أن هذه العقد لا يشترط تواجدها في مكان جغرافي واحد لكنها في الغالب تكون موزعة على أنحاء الأرض وتتقاسم الوظائف لكن في المجموع نجد أن الوظائف تكون قليلة ومركزة لأنه هنا يبحث عن الدقة في المقام الأول وهذا النوع من التعددية يخدم تطبيقات أبحاث الفضاء والمراصد الفضائية في جميع أنحاء الأرض كذلك نجد أن المنظمات التي تدير مثل هذه التطبيقات هي منظمات لا علاقة لها بالمشروع نفسه ما يفتح المجال لمفهوم Out Sourcing والهدف من وراء عدم تواجد هذه العقد في مكان واحد هو أن يكون مكان معين لهدف تخزين البيانات ومكان آخر للتحليل وآخر لجمع البيانات وهكذا نجد أن تبادل البيانات بين هذه العقد أو الأماكن يتم في حال معين وليس طول الوقت وهذا يعطي مفهوم جديد من مفاهيم اللامركزية إذ أن كل مجموعة تعمل كجزء مستقل ولا تتأثر بالمجموعات الأخرى لهذا نجد أكثر من مؤسسة في مثل هذه المشروعات.

التجربة العملية:

أتذكر انه منذ حوالي عام أو أكثر كنت مسئول عن مشروع تطوير تابع لأحدى المؤسسات التي عملت بها كان الهدف منه إيجاد مجموعة من الحلول التي تستوعب عدد اكبر من العملاء على نظام سيرفرات Asterisk والهدف الرئيسي لي وكان هذا الهدف هو التكنيكال أو التقني هو تخفيف الأحمال إلى اكبر حد وهنا لدي خياران قبل العمل احدها كان البحث أو محاولة بناء هذه الأنظمة على اليونكس وليس لينكس بينما الآخر كان عمل Cluster على اللينكس بهدف توزيع الأحمال على مجموعة من السيرفرات بالنسبة لي قد أعددت التقرير بكل أمانة وقمت بتقديمه للإدارة العليا وقامت الإدارة برفض الحل الأول وهو اليونكس وقبول الحل الثاني تحت سبب انه معروف لدى أكثر مهندسي المشروع لكن اليونكس غير معروف بالمرة وفي حال الأعطال يتهدد المشروع كله وقد كان.

عندما بدأنا في التنفيذ وتقسيم مجموعة العمل إلى مجموعات صغيرة كل منها تهتم بجزء معين قمنا بالبحث عن مجموعة من الحزم تدير هذه الخدمات وكان بينها LinuxHA – OpenSER وقد عملنا على كلاهما واختيار الأفضل، لكن في مثل هذا المشروع قد تعمقنا كثيراً جداً في الشبكات وبنية البروتوكولات والبورتات بحق كان مشروع جميل.

أتمنى من الله – عز وجل – أن تكون الإفادة وصلت، إلى اللقاء في مقالات جديدة بإذن الله.

كيفية أعطاء التصاريح على اجهزة سيسكو

بقلم: أيمن النعيمي

قد يكون موضوع التصاريح لايستخدم كثيرا في الشركات الصغيرة لكن مع الشركات الكبيرة نجد أستخدام واسع لهذا الموضوع وهو كيفية تحديد صلاحيات كل مستخدم على الروتر أو السويتش وبكلام آخر ما هي الامكانيات والأوامر التى يمكن لهذا المستخدم أن ينفذها

وقد يخطر على بالك تساؤل صغير وهو لماذا في الشركات الكبيرة فقط ؟ أنا طبعا لم أعني أن هذا الموضوع لايمكن أستخدامه في الشركات الصغيرة لان الفكرة ببساطة لو كان لدينا شركة صغيرة فالمشرفين على هذه الأجهزة لن يكونوا كثيرين فقد يكونوا واحد أو أثنين فقط لذا فالمخاطر أقل لكن لو نظرنا إلى الشركات الكبيرة مثل شركات الأنترنت لو وجدنا أن هناك الكثير من المهندسين المشرفين ومنهم من لديه خبرة كبيرة ومنهم من هو مبتدئ في هذا المجال لذا يجدر تحديد صلاحيات هذه النسبة من المهندسين لأن أي خطأ ولو كان بسيط قد يردي إلى مشاكل نحن في غنى عنها لذا أحرص على هذا الموضوع كثيرا.

وقبل أن أبدا لنتفق على بعض الامور الهامة والبسيطة

By default على الروتر هناك 15مستوى للصلاحيات

-الصلاحية رقم 0هي لـ exec mode وفيها يتاح خمس أوامر فقط disable, enable, exit, help, andlogout والصلاحية رقم 1 وهي وضعية الـDefault لـ User EXEC mode والصلاحية 15هي لـ Privilege mode

-يجب ان يكون هناك كلمة سر على الروتر تحمل الصلاحية 15والتى عادة تكون من خلال enable secret

-الصلاحيات من 1إلى 14هي الصلاحيات التخصيصية customize level والتى سوف نعمل عليها

-عند عمل صلاحية جديدة يجب ان يكون لها كلمة سر

لنبدأ الآن أستعراض كيفية عمل صلاحيات محددة سوف ندخل على الروتر ونتوجه إلى الـ Configuration Mode ونقوم بكتابة الأمر التالي :

```
Cisco's IOS
Router(config)#privilege (exec,configure)level (0-15) command
```

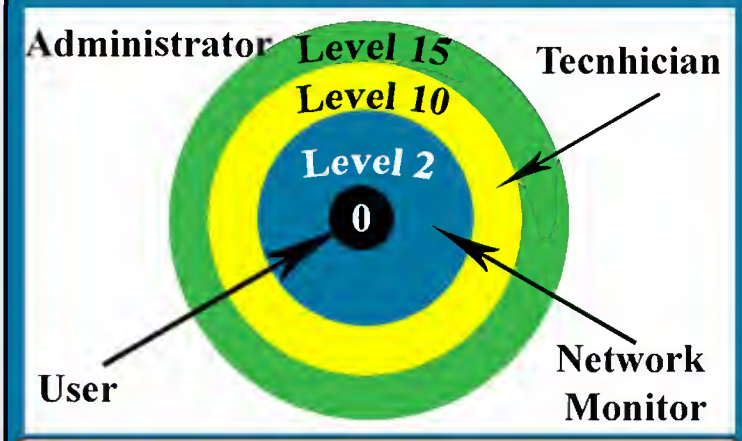
في هذا الأمر نقوم بتحديد أولا ماهو الأمر الذي أريد أن أسمح به فلو كان الأمر سوف يكتب في وضعية الـ Exec عندها سوف أضع هذه الكلمة وبعدها احدد رقم المستوى وآخيرا أكتب الأمر الذي أريد أن أسمح لهذا الشخص بتنفيذه في هذه الوضعية وهذا مثال توضيحي

```
Cisco's IOS
Router(config)#privilege exec level 3 show running-config
```

يتضح لكم من هذا المثال أني حددت رقم المستوى بثلاثة وفيها أسمح للأشخاص الذين يدخلون على هذا المستوى بتنفيذ أمر show running-config وقبل أن تذهب لتجربة الامر لن تنسى أن نضع كلمة سر لهذا المستوى كما أوضحت في البداية وصيغة الامر سوف تكون على الشكل التالي

```
Cisco's IOS
Router(config)#enable secret level 3 networkset
```

وقد خصصت كلمة networkset لكي تكون كلمة السر لهذا المستوى من الصلاحيات وبقى علينا شيء واحد أن نحفظ الأعدادت و نخرج من الروتر ونعاود الدخول لكن هذه المرة سوف لن نكتب الأمر enable وحيدا بل يجب أن نتبعه برقم المستوى أي نكتبه بهذا الشكل




```
Cisco's IOS
Router>enable 3
```

وبالتالي سوف تنطبق عليك الصلاحيات الموضحة بهذا المستوى وهو صلاحيات المستوى 0بالأضافة إلى صلاحيات الرقم 3وهي أمكانية عرض الأعدادات الموجودة على الروتر ولو حاولنا أن نكتب الأمر show interface على الموجه الاوامر سوف يظهر لنا خطأ بأن هذا الأمر غير موجود ولو حاولت الدخول إلى الـ con-figure mode سوف يقابل بالرفض أيضا لذا لنعد ونقوم بأتاحة هذان الأمران

```
Cisco's IOS
Router(config)#privilege exec level 3 configure terminal
Router(config)#privilege exec level 3 show interfaces
```

نحفظ الأعدادت وندخل مرة ثانية على المستوى الثالث لنجد أن هذه الأوامر أصبحت متاحة ولو في حال قمنا بكتابة أي أمر في الـ configure mode سوف يقابل أيضا بالرفض مثل ان نكتب interface fastethernet 0/0والسبب طبعا لان المستوى لم يتم التصريح له بأستخدام وكتابة أي أمر هناك لذا لنقم بعمل تصريح يسمح للمستخدمي هذا المستوى من الدخول على المنافذ وأعطائهم أيبي

```
Cisco's IOS
Router(config)#privilege configure level 3 interface
Router(config)#privilege interface level 3 ip address
```

لاحظ معي ان الأمر الأول سمحت فيه بكتابة الأمر interface في الـ configu-re mode بينما سمحت بالأمر ip address في الـ Interface mode وبالتالي صاحب هذه الصلاحيات سوف يتمكن من تغيير الأيبي لكن لن يتمكن من تفعيل المنفذ لانه ببساطة لايملك صلاحية الأمر no shutdown

الخلاصة : الصلاحيات من 0إلى 14هي مستويات غير مدعومة من أي شيء ماعدا الصفر وقد وضحت ماهي الأوامر التى تدعمها والمستوى واحد هو المستوى الـ default لأي مستخدم لذا أي مستوى أعلى من مستوى الواحد يأخذ نفس صلاحيات المستوى الذي تحته وهذا يعني أن المستويات من 2إلى 14سوف تحصل على صلاحيات المستوى رقم واحد لذا لو قمت بأعطاء المستوى رقم أثنان صلاحية كتابة الأمر show interface سوف يكون له صلاحيات المستوى رقم واحد زائد صلاحية كتابة الأمر show interface ولو رحت عملت للمستوى رقم 3صلاحيات الدخول إلى configure mode عندها سوف يحصل على صلاحيات المستوى رقم واحد وعلى صلاحيات المستوى رقم أثنان وهي أتاحة أستخدام الأمر show interface بالأضافة إلى الصلاحيات المعطاة له من قبل المدير وهي الدخول إلى الـ configure terminal وهكذا حتى نصل إلى المستوى و14لاحظ أيضا أن المستوى صفر وواحد يمكن التعديل عليهم أيضا وأضافة أوامر جديدة له

قسم أمن وحماية الشبكات

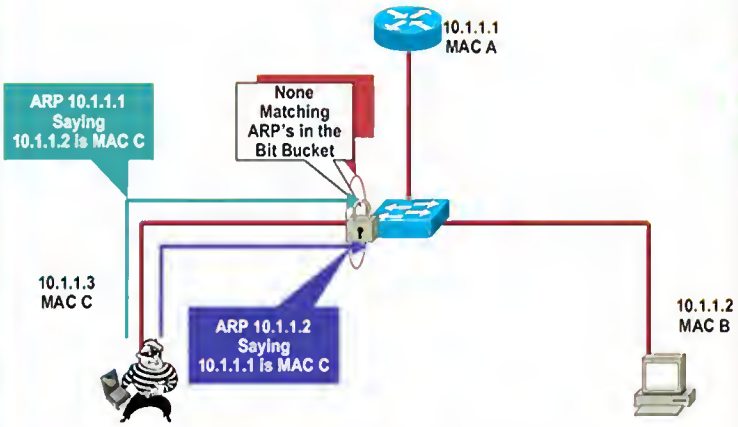
هذا القسم سوف يتم عرض فيه كل الأمور الواجب عملها في الشبكة بهدف التخفيف من نسبة القرصنة التى تحدث على الشبكة وأرجو منك أن تدقق على كلمة تخفيف لان النظرية العامة تقول لايوجد جهاز أمني خالي من الثغرات مهم كانت قوته!

هجوم الـ ARP Spoofing وكيفية التصدي له ؟

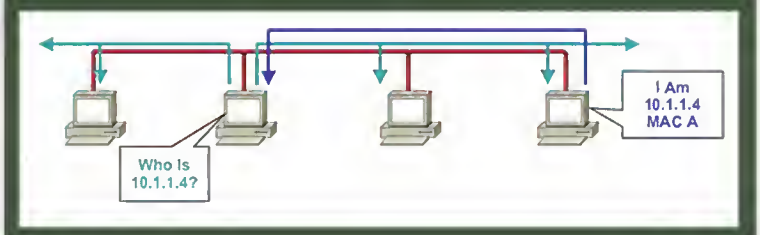
بقلم: أيمن النعيمي

قدمة

قبل أن يبدأ أي جهازان موجودان على الشبكة الأتصال فيما بينهم يتوجب على كل واحد منهم أن يعلم العنوان الفيزيائي الخاص بالآخر والذي نعرفه بي الماك أدريس لذا ومن هذا السياق تم إيجاد بروتوكول خاص بهذه العملية ويدعى ARP Protocol وظيفة هذا البروتوكول هي أرسال طلب ARP Request إلى الشبكة على شكل Broadcast يسأل فيها عن العنوان الفيزيائي لأيبي معين يريد الأتصال معه وبدوره ينتشر هذا الـ Broadcast على كل الشبكة حتى يصل إلى وجهته المقصودة (الأيبي) وعندما يصل هذا الطلب يرد عليه الجهاز المقصود بالماك أدريس الخاص فيه على شكل ARP Replay لكن

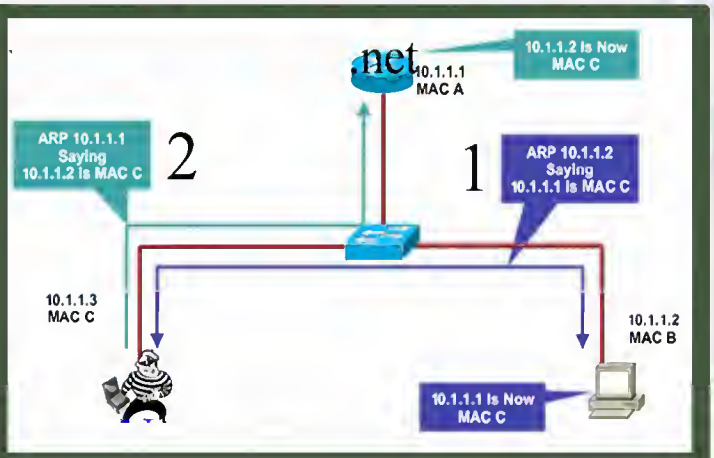


بالماك أدريس الخاص فيه على شكل ARP Replay لكن هذه المرة يكون الرد Unicast وبتلك الطريقة يبدأ الجهازان التواصل مع بعضهما البعض وهذه صورة توضيحية لسير العملية :



فكرة الهجوم

دائما ما تكون فكرة الهجوم هي أبسط شيء في عملية الأختراق فبعد وصول الرد من الجهاز يتم حفظ هذا الماك أدريس والأيبي الخاص به في جدول يدعى الـ Arp Table حتى لو في حال أراد الأتصال معه مرة أخرى يتم الرجوع إلى الجدول وهي عادة تكون مؤقتة تزول مع عملية أغلاق جهاز الكمبيوتر ومن هنا يبدا المخترق هجومه اللعين فهو ببساطة يقوم بأرسال ARP Replay مزور لأحد الأجهزة الموجودة على الشبكة معلما أياه بأن الماك أدريس الخاص بأحد الأيبيات عنوانه كذا وكآن الموضوع تم من خلال طلب من الجهاز المراد أختراقه والنتيجة سوف تكون التعديل على جدول الـ ARP وتغيير العنوان الفيزيائي لأحد الأيبيات والتى عادة ما تكون الـ Gateway الخاص بالشبكة لذا ومن هذا المنطلق يبدأ الجهاز المخترق بأرسال بياناته وطلباته إلى جهاز المخترق وكأنه هو الروتر ومن ناحية المخترق كل مايقوم به هو أعادة توجيه هذه البيانات إلى وجهتها الحقيقية أي إلى الروتر مستغلا مرور البيانات جميعها من خلال جهازه وبالتالي تمكن من تحويل جهازه إلى MITM وسوف يتمكن من مشاهدة وقراءة كل الترافيك العابر من الجهاز المخترق إلى الروتر وطبعا المخترق لن ينسى أن يرسل طلب مزور آخر إلى الروتر معلما أياه بأن العنوان الفيزيائي للجهاز المخترق هو أيبي الجهاز الخاص به لنشاهد هذه الصورة التوضيحية أولا :



الأدواة المستخدمة في الهجوم

لهذا النوع من الهجمات الكثير من الأدوات وأشهرها أداة dsniff ,ettercap وطبعا البرنامج الذي يزعج الكثير من مشتركي الانترنت netcat وأن كان لايقوم بتنفيذ مثل هذا النوع من الهجوم لكن فكرته واحده وهي قطع الأنترنت عن المستخدمين من خلال تغيير العنوان الفيزيائي لـ Gateway والخ.... وأغلب هذه البرامج لاتحتاج إلى أحترافية في الأستخدام مجرد بضع ضغطات وينتهي الأمر.

الحماية من هذا النوع من الهجمات

على مستوى المستخدم: لحمايتك من هذا النوع من الهجمات الخبيثة يفضل دائما أن تقوم بعمل Static ARP لـ Gateway الخاص بالشبكة وقد تحدثت عن هذا الموضوع بالتفصيل الممل في العدد السابق من المجلة وفيه شرحت كيفية أعدادها على أجهزة سيسكو وجونيبر ومايكروسوفت ولينوكس لذا أحرص دائما على القيام بهذا الأمر لو شككت بالأشخاص الموجودين معك على الشبكة .

ولو في حال اردت الأتصال بأحد الأجهزة أو سيرفرات الموجودة على السيرفر عن بعد بأن تستخدم الـ SSH كخيار يؤمن لك سرية كاملة لكل بياناتك لو في حال تم أعتراضه من قبل أحد المخربين

وهناك بعض الأدوات الأحترافية التى تساعدك في عملية مراقبة الترافيك الخاص بالشبكة وأخص بهم برنامج Snort وبرنامج XARP والذي يؤدي وظيفة مهمة جدا وهي مراقبة عملية الـ Mapping التى تحدث على الـ ARP Cache .

على مستوى الشبكة : قدمت سيسكو لمثل هذا النوع من الهجمات خاصية تدعى AID(dynamic ARP inspection) والتى يشترط تفعيلها على السويتش تفعيل خاصية الـ DHCP Snooping التى تحدثنا عنها في أحد الأعداد السابقة .

كيف تعمل خاصية الـ DAI

تعتمد هذه الخاصية كما ذكرت على وجود خاصية الـ DHCP Snooping فعند تفعيل خاصية الـ DAI يلجأ هو بدوره إلى الجدول الخاص بي الـ DHCP Snooping لكي يتأكد ويصادق على الـ ARP Packet الواصلة إلى السويتش من خلال المنفذ المخصص له وبكلام آخر عندما يتم توزيع الأيبي على الأجهزة يقوم الـ DHCP Snooping بعمل جدول يوضح الأيبي الذي تم أرساله من سيرفر الـ DHCP ويربطه برقم المنفذ والماك أدريس الخاص فيه وهذه صورة توضيحية للجدول

```
sh ip dhcp snooping binding
MacAddress          IpAddress       Lease(sec)  Type           VLAN  Interface
------------------  --------------  ----------  -------------  ----  --------------------
00:03:47:B5:9F:AD   10.120.4.10     193185      dhcp-snooping  4     FastEthernet3/18
00:03:47:C4:6F:83   10.120.4.11     213454      dhcp-snooping  4     FastEthernet3/21
```

والذي يستفيد منه الـ DAI لكي يتأكد من أن الـ ARP Packet مطابقة لهذه المعطيات .

الأعدادات

Cisco's IOS
```
Switch >en
Switch #conf t
Switch(config)# ip arp inspection vlan 10
```

ولو في حال Vlan أرجو أن تلاحظ أن تفعيل هذه الخاصية يتم على مستوى الـ Vlan مثل 10,11,12, نضع فاصلة ونكتب باقي الـ Vlan أردنا ضم أكثر من 25,112,300 وآخيرا نقوم بكتابة الأمر التالي على المنافذ المتصلة مع اجهزة موثوقة مثل سويتشات آخرى على سبيل المثال

Cisco's IOS
```
Switch >en
Switch #conf t
Switch(config)#interface fastethernet 0/0
Switch(config)# ip arp inspection trust
```

وللتأكد من حالة المنافذ والخاصية

Cisco's IOS
```
show ip arp inspection statistics vlan 10
```

Storm Control أحمي شبكتك من هجمات الـFlood

بقلم: أيمن النعيمي

Storm Control خاصية مفيدة وهامة لحماية الشبكات من هجمات الـ Flood التى من الممكن أن تتعرض لها الشبكة من خلال هجوم مايعرف بي الـ denial-of-service وفكرة الخاصية ببساطة هي مراقبة الترافيك الذي يدخل من خلال كل منفذ موجود عندنا على السويتش.

كيف تعمل خاصية الـStorm Control ؟

تقوم هذه الخاصية الموجودة في سويتشات سيسكو بمراقبة الترافيك الداخل إلى السويتش وأقصد بكلمة الترافيك الأنواع الثلاثة المعروفة وهي Unicast, Broadcast, Multicast وذلك من خلال تحديد نسبة مئوية معينة تقوم أنت بتحديدها وهذه النسبة تمثل حجم الترافيك الذي يمر في ثانية واحدة بحيث لوتجاوز هذا البورت الحد المسموح له)النسبة المئوية التى قمنا بتحديدها (فسوف يقوم بعمل ردة فعل سوف نحددها نحن وسوف أتكلم عنه في مرحلة الأعداد كما تفيدنا هذه الخاصية في تحديد النسبة المئوية لكمية الباندويث الذي يعبر عن المنفذ لان في حال زيادة نسبة الـunicast مثلا عن النسبة المسموح بها فسوف يقوم المنفذ بعمل Drop بشكل أوتماتيكي للترافيك ولن يسمح للترافيك للعبور إلا بعد أن يصل حجم الترافيك إلى نسبة مئوية نقوم نحن بأعداداها أيضا

ملاحظة هامة: كل أنواع الـBroadcast & Multicast ترافيك سوف يتم مراقبتها بأستثناء الترافيك الخاص بي الـ BPDU Frame and CDP حتى الترافيك الخاص بي OSPF & EIGRP سوف يتم مراقبته والمقصود طبعا الـ Multicast الذي يتم بين الروترات

كيف أعداد الـStorm Control ؟

كما أتفقنا في بداية الموضوع أن أعداد الـ Storm Control يتم من خلال تفعيله على كل منفذ موجود على السويتش والخطوات هي كالتالي :

Cisco's IOS
```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# storm-control unicast level 87 65
```

في هذا المثال قمت بتحديد النسبة الاعلى rising suppression التى أريد أن أسمح بها لي Unicast للعبور من خلال منفذ الجيجا أيثرنت بحيث لو تجاوز نسبة الـ 87% فأن البورت سوف يبدأ بعمل Drop للباكيت حتى تصل إلى النسبة الصغرى 65 falling suppression% في الثانية ولاحظ أيضا أني لم أقم بتحديد ردة فعل لان ردة الفعل الطبيعية هي فلترة الترافيك بحسب النسب الموضحة ولو أردت أن أضع ردة فعل سوف أزيد سطرا آخر إلى الأعدادات وهو

Cisco's IOS
```
Switch(config-if)# storm-control action shutdown | trap
```

لنشاهد مثال آخر

Cisco's IOS
```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# storm-control broadcast level 20
Switch(config-if)# storm-control action shutdown | trap
```

في المثال الثاني قمت بتحديد نسبة الـBroadcast المسموح له بي 20% ولو في حال تم تجاوز هذا الحد فان البورت سوف يقوم بعمل ردة فعل وهي نوعين :

الأولى هي Shutdown وطبعا سوف تقوم الخاصية بأغلاق المنفذ بشكل أوتماتيكي ,أما الثانية هي Trap وهي لأرسال SNMP trap إلى الـAgent للأعلام عن زيادة النسبة المسوح بها

مع العلم لو أنني قمت بوضع النسبة 0 فهذا يعني أنني سوف أمنع الـ Broadcast بشكل كامل عن المنفذ ولو أخترت النسبة 100 فهذا يعني أنني لن أخضع الـBroadcast للمراقبة

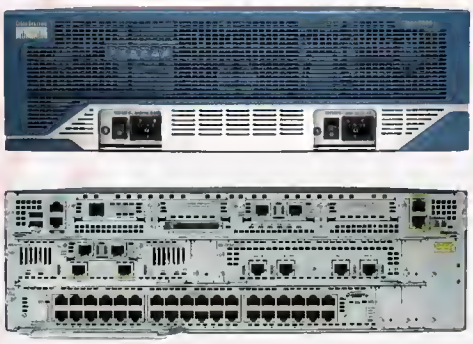
وآخيرا نستخدم الإمر Show Storm-control لعرض حالة البورتات

عتاد و معلومات

أعداد: أيمن النعيمي

Cisco Systems

RAM	512 MB (installed) / 1 GB (max) - DDR SDRAM
Flash memory	128 MB (installed) / 512 MB (max)
Type	Router
MAX Transfer Rate	1 Gbps
Encryption Algorithm	DES, Triple DES, SSL, 128-bit AES, 192-bit AES, 256-bit AES
Supplied OS	Cisco IOS Advanced IP services
Digital Signaling Protocol	Wired
DCP	Ethernet, Fast Ethernet, Gigabit Ethernet
Protocol Remot	SNMP 3, SSH-2
Interfaces	2 x network - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45 ¦ 2 x USB ¦ 1 x management - console ¦ 1 x network - auxiliary
Firewall protection, hardware compression, hardware encryption, VPN support, MPLS support, content filtering, URL filtering, QoS, Dynamic Multipoint VPN	



CISCO 3845-HSEC/K9

RAM	128 MB
Flash memory	16 MB
Ramer Table of MAC Addr	12K entries
Authentication method	Kerberos, Secure Shell(SSH),RADIUS,TACACS+
Interfaces	management-console RJ-45 2 x network stack devicet
Connection Type	Half-duplex, full-duplex
Data Rate	100 Mbps
DCP	Ethernet,Fast Ethernet 10Base-T/100Base-TX
Protocol Remote	SNMP1,RMON1,RMON2,SNMP,Telnet,SNMP3
Number of Ports	48 x Ethernet 10Base-T, Ethernet 100Base-TX
Flow control,full duplex,routing,IP-routing,DHCP support,auto-negotiation,ARP support, trunking, load balancing, VLAN support, auto-uplink (auto MDI/MDI-X),IGMP snooping,manageable,IPv6 support	

Catalyst 3750 48TS-E

RAM	256 MB (installed) / 1 GB (max)
Flash memory	64 MB (installed) / 256 MB (max)
Protocol Remote	SNMP 3
Type	Voice / fax module
Interfaces	2 x network - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45 ¦ 2 x USB ¦ 1 x management - console ¦ 1 x network - auxiliary
Encryption	DES, Triple DES, AES
Supplied OS	Cisco IOS SP services
OS Required	Microsoft Windows 98 Second Edition
DCP	Ethernet, Fast Ethernet, Gigabit Ethernet
Voice Codecs G.711, G.723.1, G.728, G.729, G.729a, G.729ab, G.726	

CISCO 2821-V/K9

Juniper NETWORKS

Aggregate Half-Duplex Throughput
* 10 Gbps

FPC Slots and Full Duplex Throughput **per Slot**
* 1 built-in, 4 Gbps additional 1 Gbps for FIC

PICs per Chassis
* 4, plus 2 additional fixed FE, or 1 fixed GE ports

Chassis per Rack
* 24

Redundancy
* No

Dimensions
* 3.5 x 17.5 x 18 in
* 8.9 x 44.5 x 45.7 cm

Mounting
* Front or center

Maximum Weight
* 38.2 lbs / 17.3 Kg

Power Options
* DC Input Power (Fully Loaded): 10 A at -48 VDC; 378 watts
* No. of power supplies required (non-redundant/redundant): 1/2
* AC System Input Power (Fully Loaded): 4 to 2 A; 100 to 240 VAC; 47 to 63 Hz; 400 watts

Router M7i

Number of Interfaces*
8 mini-GBIC (SX, LX or TX), or 2 XFP 10 Gig (SR or LR)

Maximum Number of IP Addresses in Trusted Interfaces
Unrestricted

Maximum Throughput
* 10 Gbps FW
* 5 Gbps 3DES VPN

Maximum Number of Sessions
1,000,000

Maximum Number of VPN Tunnels
25,000

Maximum Number of Policies
40,000

Maximum Number of Virtual Systems
0 default, upgradeable to 500

Maximum Number of Virtual LANs
4094

Maximum Number of Security Zones
16 default, upgradeable to 1,016

Maximum Number of Virtual Routers
3 default, upgradeable to 503

Routing Protocols Supported
OSPF, BGP, RIPv1/v2

High-Availability Modes Supported
* Active/Passive
* Active/Active
* Active/Active Full Mesh

IPS (Deep Inspection FW)
Yes

Integrated / Redirect Web Filtering
Yes

NetScreen-5200

Maximum Performance and Capacity

* **Junos Software Version Support: Junos Software 9.1**
* **Firewall Performance (Large Packets): 600 Mbps**
* **Firewall Performance (IMIX): 400M**
* **Firewall and Routing PPS (64 Byte): 175, 000 pps**
* **3DES and SHA-1 VPN Performance: 140 Mbps**
* **Concurrent VPN Tunnels: 512 MB / 1 GB DRAM 256 / 512**
* **Maximum Concurrent Sessions: 512 MB / 1 GB DRAM 64 K / 128 K**
* **New Sessions/Second: 5,000**

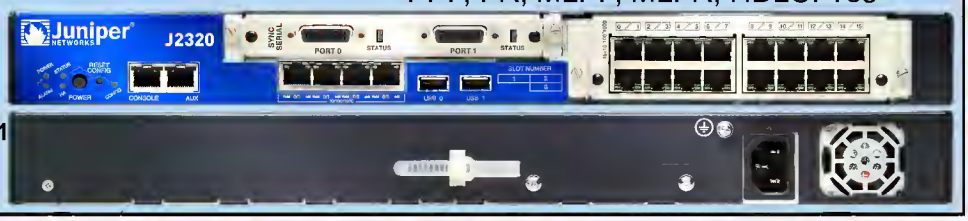
Network Connectivity

* Fixed I/O: 4 x 10/100/1000
* Maximum PIM Slots: 3
* Maximum EPIM Slots: 0

Routing, Virtualization, Encapsulations

* BGP, OSPF, RIP, Static, ECMP: Yes
* Multicast, PIM SM, SSM,IGMP: Yes
* Maximum Number of Security Zones: 40
* Maximum Number of Virtual Routers: Yes
* Maximum Number of VLANs: 256
* PPP, FR, MLPP, MLFR, HDLC: Yes

Router J2320



Data Rate
* 480 Gbps

Throughput
* 357 Mpps (wire speed)

10/100/1000BASE-T Port Densities
24 (dual-mode 1/10GbE network ports)

10GBASE-X Port Densities
24

100BASE-FX / 1000BASE-X (SFP) Port Densities
N/A

Resiliency
Dual load-sharing internal autosensing AC power supplies

Power Options
Autosensing; 110/220 VAC; 60/50 Hz

Operating System
JUNOS

QoS Queues / Port
8

Traffic Monitoring
N/A

MAC Addresses
16,000

Jumbo Frames
9216 Bytes

IPv4 Unicast / Multicast Routes
N/A

Number of VLANs
1,024

Switch EX2500

مصطلحات تقنية

إعداد: أيمن النعيمي

UNICAST : مصطلح شائع في عالم الشبكات وهو يطلق على الطريقة التى تنتقل فيها الداتا من المصدر إلى الهدف والتى تتم بأتجاه واحد ومحدد ويتم تحديد الوجهة من خلال عنوان الهدف نفسه ويستخدم في كلا الأصداران الرابع والسادس الخاص بالأيبي بروتوكول .

BROADCAST : أيضا أحد المصطلحات الشائعة جدا وهو يطلق على الطريقة التى تنتقل فيها الداتا من المصدر إلى الهدف وفيها تنتقل الداتا بكل الاتجاهات المتاحة على الشبكة مستخدمة عنوان محجوز لمثل هذا النوع من الأنتقال ويكون الايبي على الشكل التالي Destination 255.255.255.255وهي تمر عبر Hub & Switch & Bridge بينما يتوقف عند الروتر ويستخدم في الأصدار الرابع من الأيبي بروتوكول فقط.

MULTICAST : وفيه تنتقل الداتا على الشبكة ضمن ايبيات محجوزة في نطاق الكلاس D وتحمل الرانج 224.0.0.0وهو يستخدم لنقل الداتا إلى عدة نقاط معينة وفي نفس الوقت وله أستخدامات كثيرة مع الداتا الخاصة بالصوت والفيديو بالأضافة إلى أستخدامه مع بعض البروتوكولات وبالأخص بروتوكولات الـ ROUTING وهو أيضا يستخدم في كلا الأصداران الرابع والسادس الخاص بالأيبي بروتوكول .

ANYCAST : وفيه تنتقل الداتا حسب قواعد محدده من قبل المرسل مثلا أقرب جهاز على الشبكة أو أفضل مسار للداتا وهو يستخدم كثيرا مع بروتوكولات التوجيه مثل بروتوكول الـ BGP وهو يستخدم في الأصدار السادس من الأيبي .

مشاكل وحلول

سوف يتم تخصيص هذا القسم لعرض المشاكل التى قد تواجهك في الشبكة بالأضافة إلى طريقة حل المشكلة كما أرحب أيضا بأرسال مشاكلكم على بريد المجلة magazine@networkset.net للنظر فيها وتقديم أفضل الحلول لها .

سؤال: كيف أقوم بأعداد وتنصيب سيرفر خاص بي الـ **TFTP** ؟
جواب : تنصيب مثل هذا النوع من السيرفرات لايحتاج إلا شيء كل ماعليك تنصيب هذا البرنامج على جهازك وتحديد المنفذ الذي سوف يعمل عليه وانتهي الأمر .
http://tftpd32.jounin.net/tftpd32_download.html

مشكلة: عندي روتر DSL (2640u -D-link) وفيه أربعة منافذ وكل منفذ يتم وصله بكومبيوتر و بالتالي تبدأ هذه الكومبيوترات بتصفح النيت، لذلك أردت سؤالك هل هناك برنامج أو طريقة أستطيع من خلالها أن أعرف مصروف أو الترافيك الذي يصرفه كل كومبيوتر عن طريق منافذ الروتر ؟
الحل: بعد الأطلاع على مواصفات وأمكانيات المودم لم أجد هذه الخاصية متاحة أي تحديد كمية الترافيك الذي يعبر على كل منفذ لكن لو مكانك وكنت مطر إلى مراقبة الترافيك لكنت أشتريت سويتش بسيط وكرت شبكة لجهاز الكمبيوتر وربط الأجهزة الموجودة على الشبكة مع السويتش والسويتش وصلته مع كرت الشبكة الجديد ونصبت برنامج CCPROXY وحددت الترافيك لكل مستخدم أو قمت بتثبيت سيرفر مايكروتيك الذي يعطي مميزات رهيبة لمثل هذه المواضيع .

سؤال :انا حاصل على mcp,ccna وسوف استمر فى شهادات سيسكو ومايكروسفت الى اعلى مستويات الشهادة ولكنى غير حاصل على شهادة جامعية هل تغنى شهادات الشبكات عن الشهادة الجامعية للعمل كمهندس شبكات ؟
جواب: شوف السؤال هذا صعب أجيبك عليه لان هذا الموضوع هو موضوع أرزاق لكن حصولك على شهادة مثل CCIE يساعدك على حل هذه المشكلة وطبعا هناك شركات تشترط وجود شهادة جامعية .

سؤال: أنا حاصل على بكالريوس نظم ومعلومات إدارية أريد الدخول فى مجال الشبكات فبأى شئ أبدأ وأى كورسات وفى أى مكان ؟
جواب: أطلع على المجلة هناك سلسلة من المقالات حول هذا الموضوع للأستاذ عادل الحميدي

سؤال: أريد دراسة شهادة الـ Trubleshoot لكن محتار في أي كتاب أدرس إما
CCNP TSHOOT 642-832 Official Certification Guide
أو
Troubleshooting and Maintaining cisco ip networks (Student guide v1&v2)
فأيهم أشمل، بمعنى مستوعب معلومات أكثر مع أني متحيزة نوعا ما للأول ؟
جواب : الكتاب الثاني وبلا منازع فهو أقوى بكثير من الأول لكن أفضل ان تقرأ السيناريو الموجود في آخر كل جابتر من الكتاب الأول .